Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone

Patrick Ventuzelo, Olivier Le Moal, and Thomas Coudray
{patrick.ventuzelo,olivier.lemoal,thomas.coudray}@p1sec.com

P1 Security

Abstract. VoLTE (Voice over LTE) is a technology implemented by many operators over the world. Unlike previous 2G/3G technologies, VoLTE offers the possibility to use the end-to-end IP networks to handle voice communications. This technology uses VoIP (Voice over IP) standards over IMS (IP Multimedia Subsystem) networks. In this paper, we will first introduce the basics of VoLTE technology. We will then demonstrate how to use an Android phone to communicate with VoLTE networks and what normal VoLTE communications look like. Finally, we will describe different issues and implementations' problems. We will present vulnerabilities, both passive and active, and attacks that can be done using VoLTE Android smartphones to attack subscribers and operators' infrastructures. Some of these vulnerabilities are new and not previously disclosed: they may allow an attacker to silently retrieve private pieces of information on targeted subscribers, such as their geolocation.

1 Introduction

Please note:
We want to remind the reader that all passive & active tests – like the attacks described hereafter – need to be authorized by the concerned operator and competent organization.

1.1 VoLTE overview

The definition of VoLTE by the GSMA (GSM Association) is as follows:

"Voice over LTE, or VoLTE is a GSMA profile of the standards definition for the delivery of services currently provided via Circuit Switched networks – mainly voice and SMS – over the Packet Switched only network of LTE, leveraging the core network IP Multimedia SubSystem (IMS)." [1]

VoLTE technology was first deployed in Asia starting with South Korea and Singapore, at the end of 2012. It was followed by US operators like AT&T and Verizon between 2013 and 2014. Most of European operators have started the testing phase and official deployment around 2015.

In January 2016, 55 operators officially offered VoLTE features to their customers. A year later, these numbers grew to a total of 104 operators in 55 different countries. The following world map (Figure 1) is based on a GSA (Global mobile Suppliers Association) publication [2] and shows the approximate number of operators that have currently deployed VoLTE in their network as of the beginning of the year 2017.

As described, the main purpose of VoLTE implementation is to provide voice over 4G LTE networks. Moreover, subscribers using VoLTE for voice calls will get many benefits.

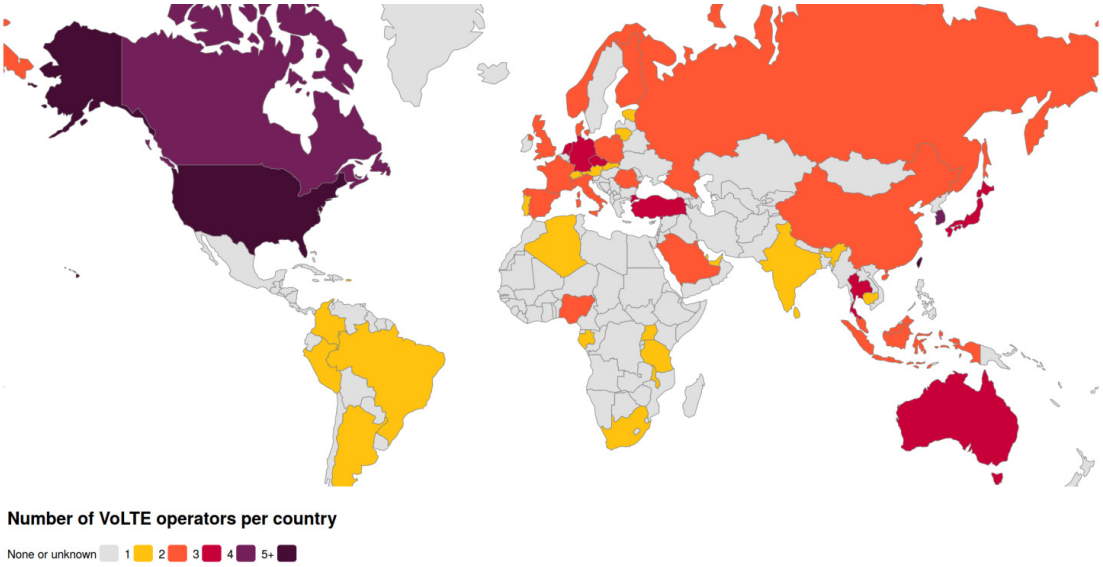

Fig. 1. World map of current VoLTE deployment

First, when using only 4G LTE for data and legacy CS networks (2G/3G) for voice with no VoLTE provisioned, Circuit Switched FallBack (CSFB) will occur when users make or receive a voice call or SMS. This CSFB technology forces the smartphone to use CS networks for calls and this is necessary due to LTE being a packet-based all-IP network that cannot support circuit-switched calls without losing data connectivity. Also, in case of loss of 4G connectivity during VoLTE calls, SRVCC (Single Radio Voice Call Continuity) has been created to permit handover between (lost) VoLTE to legacy CS network (2G/3G) and without interruption of the current voice communication.

Secondly, IMS provides higher QoS (Quality of Service) for voice service using LTE radio access technology, that means a quality for 4G calls equivalent to the one of usual 2G/3G calls.

Finally, specific codecs such as AMR-NB, AMR-WB, etc. provide a higher voice quality.

When speaking about communication between subscribers in the telecom area, we use "caller" to designate the subscriber who initiates the call and "callee" to designate the subscriber who receives it.

1.2 VoLTE Architecture

Please note:
Only the IMS architecture will be described in this part, concerning LTE architecture and EPC (Evolved Packet Core) network, please refer to "How to not break LTE crypto" [6] or 3GPP standards[1].

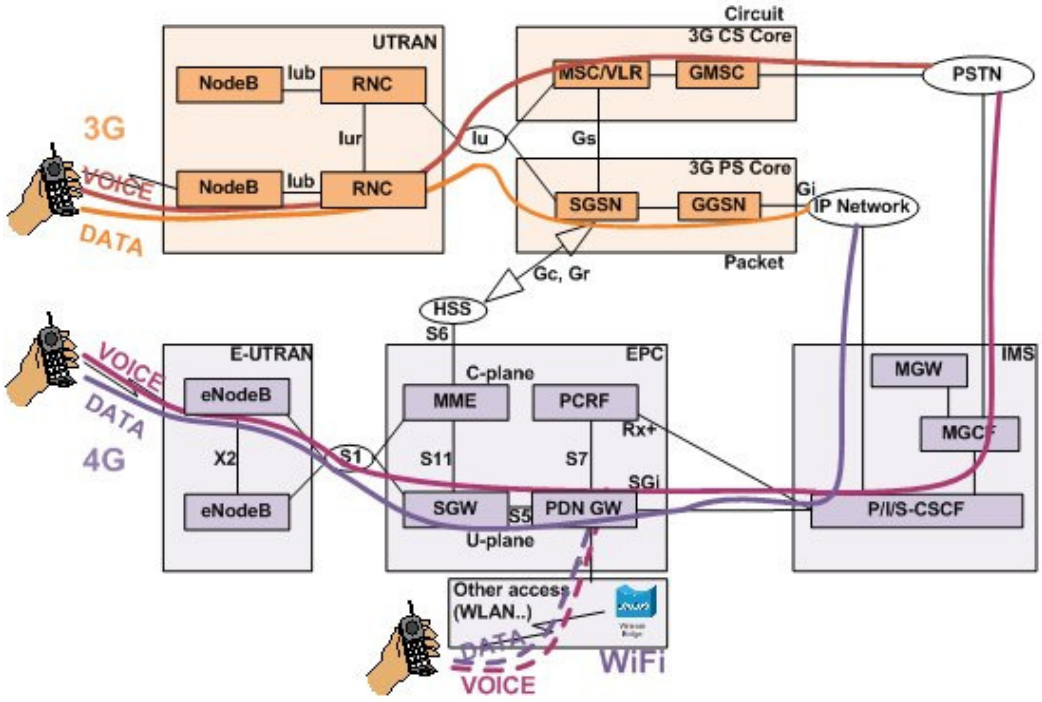

Fig. 2. Voice and Data traffic over 3G and 4G

Figure 2 shows the multiple NE (Network Elements) used for Data traffic and Voice traffic over 3G and 4G as well. The call setup necessary for VoLTE is the same as the setup for VoWiFi (Voice over WiFi), which will make future VoWiFi deployment easier for operators (WiFi part of Figure 2).

[1] `http://www.3gpp.org/specifications/`

VoLTE architecture is mainly composed of the IMS core network and IMS Services Framework (Figure 3). The IMS core network is the control infrastructure for supporting next generation IP Multimedia Services, it is mainly composed of the following network elements:

- P-CSCF: Proxy Call State Control Function
- I-CSCF: Interrogating Call State Control Function
- S-CSCF: Serving Call State Control Function
- HSS: Home Subscriber Server
- AS: Application Server
- MGW: Media Gateway Function

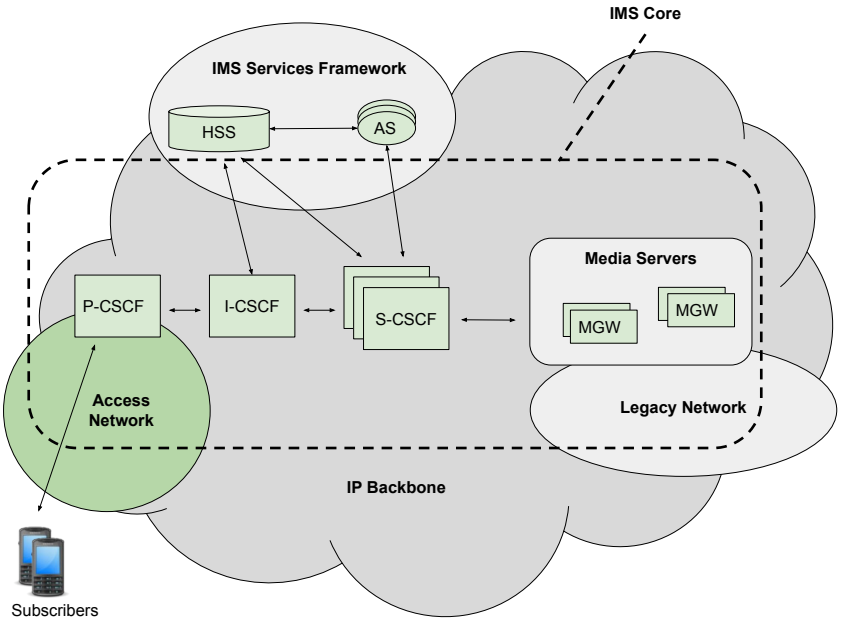

Fig. 3. Simplify VoLTE architecture

P-CSCF (Proxy Call Session Control Function): The P-CSCF is the proxy server for user equipment communications to the IMS network. It is the initial point of contact for VoLTE signaling coming from UE (User Equipment). Its main function is to forward all messages between the UE and the IMS core network, while maintaining the security associations.

The call flows related to IMS core registration between the P-CSCF and the UE is described in Section 3.1 “IMS core registration” on page 365.

I-CSCF (Interrogating Call State Control Function): The I-CSCF serves two main purposes. In case of an unregistered subscriber, its goal is to forward the initial SIP (Session Initiation Protocol) request to the suitable S-CSCF that will handle the request for registration. To find out the suitable S-CSCF, the I-CSCF will ask directly the HSS (Home Subscriber Server).

S-CSCF (Serving Call State Control Function): The S-CSCF is a SIP server providing all session management, i.e. functions like session set-up, session tear-down, session control and routing functions. It is the network element responsible for the registration of users in the IMS network.

HSS (Home Subscriber Server): The HSS is the combination of the HLR (Home Location Register) and the AuC (Authentication Center) if we compare it to 3G architecture. The HLR entity of the HSS contains all information related to the subscribers (user profiles). The HLR/HSS provides details of the subscribers to other network entities. These informations can be:

- IMS Private and public identity (IMPI/IMPU)
- Globally Routable User Agent URI (GRUU)
- International Mobile Subscriber Identity (IMSI)
- Mobile Subscriber ISDN Number (MSISDN)
- Subscriber services profiles
- Services triggers
- ...

The AuC entity of the HSS is responsible for generating authentication vectors, specific for each user. They are based on pre-shared keys, stored both in the AuC on the network side and on the user side in the SIM card.

AS (Application server): In case of VoLTE, the main Application Server is used for voice and video telephony. This application server is called TAS (Telephony Application Server) or MMTel (Multimedia Telephony) and is responsible for all services (involving both signaling and media manipulation) such as local number portability, free-call routing resolution, unified messaging and conference bridge services.

1.3 Bearers, QoS and QCI

Bearer is a virtual concept used to define the "communication channel" with a set of specific network parameters and treatments for the type of data received by the network.

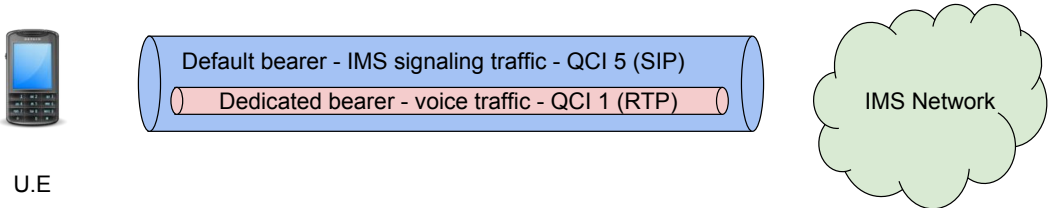

Fig. 4. Default and dedicated bearers in VoLTE

The EPC sets up one EPS (Evolved Packet System) bearer, for any LTE UE attached to the network for the first time, by default. This bearer is known as a default bearer and is used to connect the UE to a packet switched network. Thanks to the default bearer, every UE has one dedicated IP address that is a data channel used for 4G internet communication, such as web-browsing.

In case of VoLTE provisioned SIM cards, the UE will receive two other bearers: another default and a dedicated bearer. The other default bearer (the external blue pipe in Figure 4) is used for IMS signaling (SIP signaling message). As the UE will be directly connected to the IMS core network, the UE receives another specific IP address. This IP address will be used for both the default signaling bearer and for the dedicated one – used for VoLTE audio traffic (the internal pink pipe in Figure 4).

The main difference between these bearers are their QoS (Quality of Service) Class Identifier (QCI) parameters. The default bearer used for IMS signaling has a QCI of 5. That means that all the data transported over this bearer, have the maximum priority rate possible (priority 1) and a light packet delay (100 ms). Regarding the voice bearer (the dedicated bearer), it has the second maximum priority rate possible (priority 2) and a light packet delay (100 ms).

1.4 IMS protocols

From the UE's perspective of the IMS subsystem, the major protocols are: Session Initiation Protocol (SIP), Session Description Protocol (SDP), Real-time Transport Protocol (RTP) and IP/IPsec, depending on the

operator's network maturity (Figure 5). The Diameter protocol is also used between different entities of the IMS core network, but transparently for the user equipment.

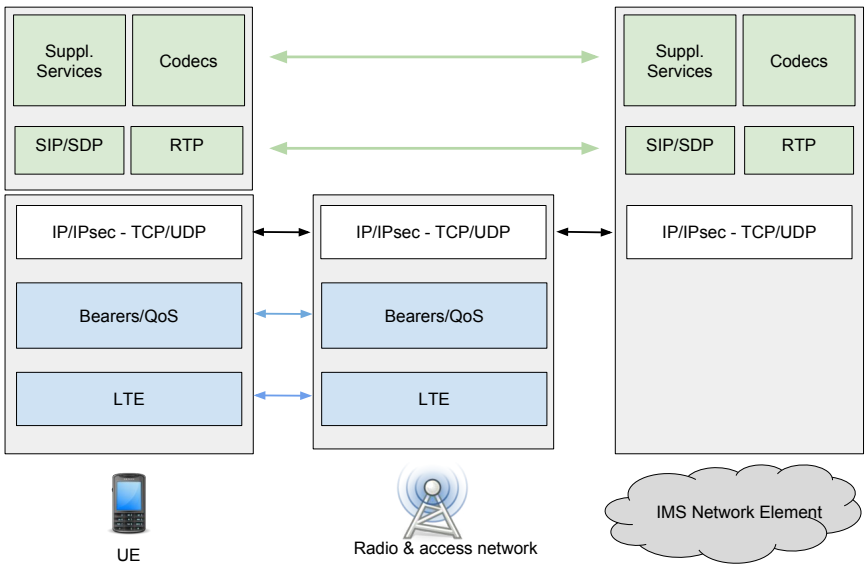

Fig. 5. UE/Network IMS Profile protocols

SIP (Session Initiation Protocol): SIP is the protocol used for all IMS signaling traffic between a UE and the IMS core network, for VoLTE communication. SIP is defined in the IETF's RFC 3261[2], it is a sequential (request/response) protocol where requests are initiated by UEs.

Most common SIP methods are *REGISTER*, *PRACK*, *INVITE*, *ACK*, *UPDATE*, *BYE* and *CANCEL*. Most common SIP response codes are as follows:

- 100 Trying
- 180 Ringing
- 183 Session Progress
- 200 OK
- 401 Unauthorized
- 403 Forbidden

More details about SIP and VoLTE call flows are described in Section 3 "SIP communication" on page 365.

[2] `https://tools.ietf.org/html/rfc3261`

SDP (Session Description Protocol): The Session Description Protocol (SDP) is the protocol used to inform the callee (B-party) about media parameters that the caller (A-party) is able to handle. This protocol is similar to a media parameters negotiation protocol, without any possibility for the callee, to propose his own parameters. These parameters are mainly composed of media information such as: media type, speech codec, IP address and ports (UE-A, UE-B, IMS-MGW), that will be used to establish the UE's dedicated bearer. The following example (Figure 6) shows the most interesting values contained in the SDP header field of VoLTE *INVITE* message.

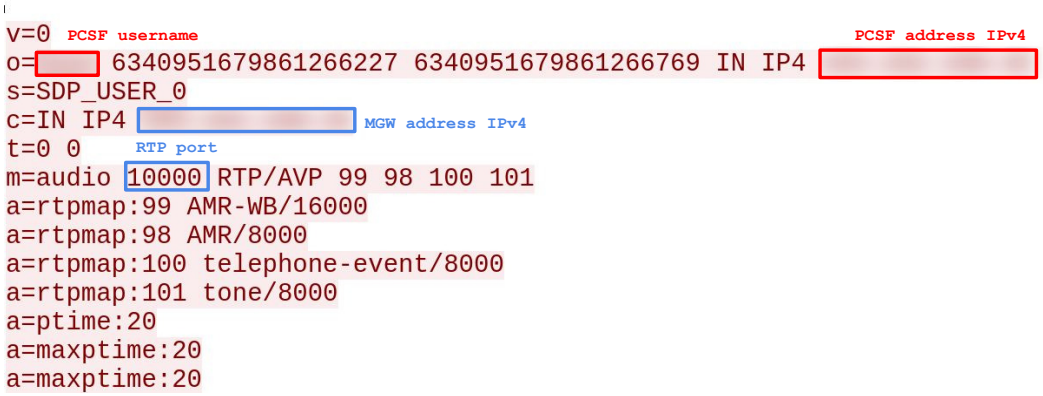

Fig. 6. Interesting values in SDP header

RTP (Real-time Transport Protocol): RTP protocol is used to transport audio and video data over IP (usually over UDP). In VoLTE communications, this protocol is used over the dedicated bearer between the UE and the Media GateWay (MGW). All the parameters regarding the codec used to encode the audio data are present in the received SIP packet, during UE registration (more specifically in the SDP part of SIP packets)

IPsec: Some operators use IPsec for their VoLTE network, for SIP communication between the UE and the P-CSCF. This IPsec tunnel is used to encapsulate all SIP default bearer traffic.

IPsec can be used in two modes: in transport mode, the IPsec header encapsulates the IP payload, while in tunnel mode, the origin IP datagram is encapsulated into a new IP header. In VoLTE, ESP mode is used in transport mode. Hence, the IPsec ESP header encapsulates the IP payload, meaning that the original IP datagram is therefore secured.

2 VoLTE implementations in Android

This chapter will describe different implementations of the VoLTE technology for Android UE and the techniques that can be used to directly interact with the operator's IMS core network.

2.1 Vendor implementation

VoLTE implementation on Android heavily relies on vendors of chipsets like Qualcomm, Mediatek, Exynos but also depends on product applications like VoLTE/RCS clients. When VoLTE is enabled on Android phones, the RMNET virtual ethernet driver sets up an interface on phone. It can usually be found under the name *rmnet1* when listing interfaces available on the phone. This interface is used for user-data transfer to the baseband.

On some tested implementations (e.g. Samsung S6), this interface is actively used by Android-side components to perform the SIP communication along with the IPsec security associations setup. As seen in the next section, a user can easily eavesdrop on this interface to access signaling and media content, and access to the IPsec Security Associations (SA) directly on the Linux Kernel IPsec stack (also known as *Netkey*).

On other tested implementations (e.g. Xperia phones), the *rmnet1* interface does not leak any IMS traffic from/to the UE. Also, IPsec SA are not visible from the Kernel side. Most of the work has to be achieved by the Qualcomm chipset itself, on a lower layer. Another way to eavesdrop on this kind of implementation, is to use the diagnostic device (*/dev/diag*) available on the phone, with proprietary debug tools (QXDM).

It seems obvious after a quick survey that there is no standard that defines VoLTE implementation on Android, and not all implementations are equivalent in terms of security. A large field of security research is waiting to be exploited.

2.2 Traffic eavesdropping and injection

All the SIP signaling traffic is sent to the P-CSCF via the default bearer negotiated when the UE registered itself to the operator network. In this part, we will see how to sniff traffic and communicate directly with the P-CSCF.

On Samsung S6, as seen previously, a pseudo-interface named as *rmnet1* is created once the bearer is established. A rogue application or a curious user with root privileges and traffic sniffing tool such as *tcpdump*, can sniff SIP traffic going through this interface and analyze the resulting

pcap by using Wireshark and the IPsec encryption key negotiated between the UE and the IMS core network.

Depending on the network operator's architecture, IPsec tunnels between the UE and the IMS core network will be set up. In this case, we need to inject data directly into this existing IPsec tunnel, typically, when we want to test active vulnerabilities and replay traffic. The easiest way to achieve this is to reuse an existing socket used by a legitimate IMS service on Android. Reusing this socket will permit to inject traffic inside the IPsec tunnel, as the association already was established by the Linux Kernel IPsec stack (*Netkey*).

The SPD (Security Policy Database) contains rules that tell the implementation, how to process datagrams. It can be displayed with the *ip xfrm policy* command (Figure 7).

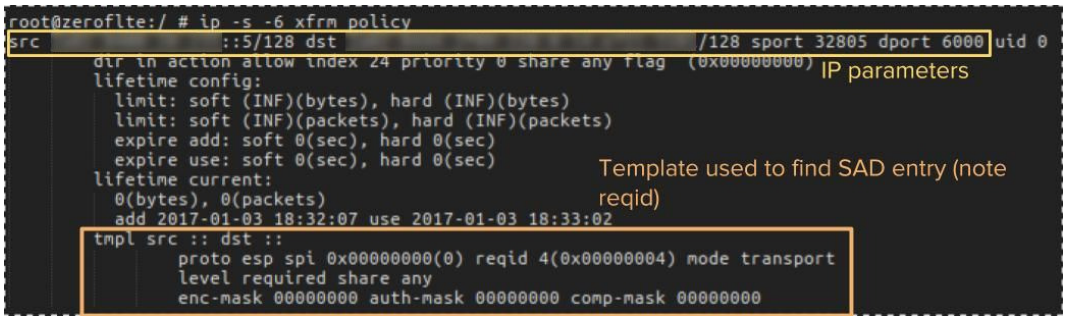

Fig. 7. Security Policy Database

The SAD (Security Association Database) contains a set of security information that describes a secure connection. It can be displayed with the *ip xfrm state* command (Figure 8).

The keys retrieved can be used to decrypt eavesdropped traffic when doing passive recognition.

Another way to inject traffic is to reimplement the SIP call flow for the registration with the P-CSCF and a custom application. A strong requirement is to be able to query the USIM card for authentication. This can be done using an external SIM card reader. IPsec parameters (ciphers for encryption and authentication) are also negotiated during the SIP registration phase.

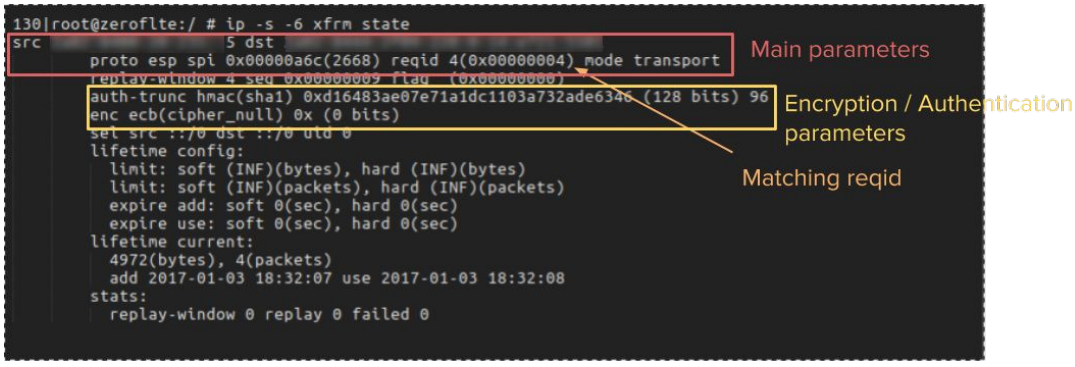

Fig. 8. Security Association Database

3 SIP communication

In this chapter, we will see the basic call flows from a subscriber's UE point of view. In the first part, we will describe the IMS core registration and in the last part we will depict the different exchanges made during a communication, between two smartphones (UE-attacker to UE-victim).

3.1 IMS core registration

Please note:
We will not describe all the mechanisms involved in this call-flow. For more information, please visit the following links:

- *eventhelix*[3]
- *hongjoo71 blogspot*[4]
- *simpletechpost*[5]

The registration between the user equipment (UE) and the IMS core network is mandatory to allow the creation of the two bearers (default signaling bearer and dedicated voice bearer). This registration, described in Figure 9, involves a challenge-response authentication mechanism using data shared by the HSS (AuC component) and the UE SIM card (AKA-MD5 challenge with RAND and AUTN parameters).

The registration phase starts after the reception of a SIP *REGISTER* message, from an unauthenticated user by the IMS core network's entry point i.e. the P-CSCF (Figure 10).

[3] `http://www.eventhelix.com/ims/registration/`
[4] `http://hongjoo71-e.blogspot.fr/`
[5] `http://www.simpletechpost.com/`

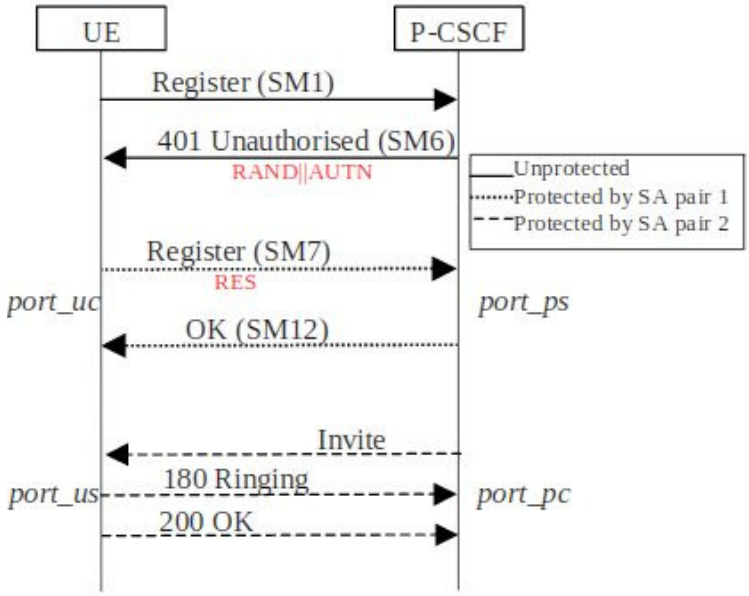

Fig. 9. SIP Registration

```
1  REGISTER sip:ims.mnc042.mcc123.3gppnetwork.org SIP/2.0
2  Content-Length: 0
3  Via: SIP/2.0/UDP [{UE_ip}]:5060;branch=c7dH8567G276;transport=UDP;
       rport
4  User-Agent: IM-client/OMA1.0 Samsung/SM-G920F-XXU2BOFJ Samsung-RCS
       /5.0
5  Supported: sec-agree,path,gruu
6  Proxy-Require: sec-agree
7  Require: sec-agree
8  Contact: <sip:{UE_IMSI}@[{UE_ip}]:5060;transport=UDP>;q=1.00;+g.3gpp
       .icsi-ref="urn;urn-7;3gpp-service.ims.icsi.mmtel";+g.3gpp.smsip;
       video;+sip.instance="<urn:gsma:imei:{UE_IMEI}>"
9  Max-Forwards: 70
10 CSeq: 1 REGISTER
11 Call-ID: 2357994989@{UE_ip}
12 To: <sip:{UE_IMSI}@ims.mnc042.mcc123.3gppnetwork.org>
13 From: <sip:{UE_IMSI}@ims.mnc042.mcc123.3gppnetwork.org>;tag
       =653963826
14 Security-Client: ipsec-3gpp;prot=esp;mod=trans;spi-c=3976;spi-s
       =3977;port-c=5202;port-s=6000;alg=hmac-sha-1-96;ealg=null
15 Authorization: Digest username="{UE_IMSI}@ims.mnc042.mcc123.3
       gppnetwork.org",realm="ims.mnc042.mcc123.3gppnetwork.org",uri="
       sip:ims.mnc042.mcc123.3gppnetwork.org",nonce="",response="",
       algorithm=AKAv1-MD5
16 Expires: 3600
```

Listing 1. SIP REGISTER message

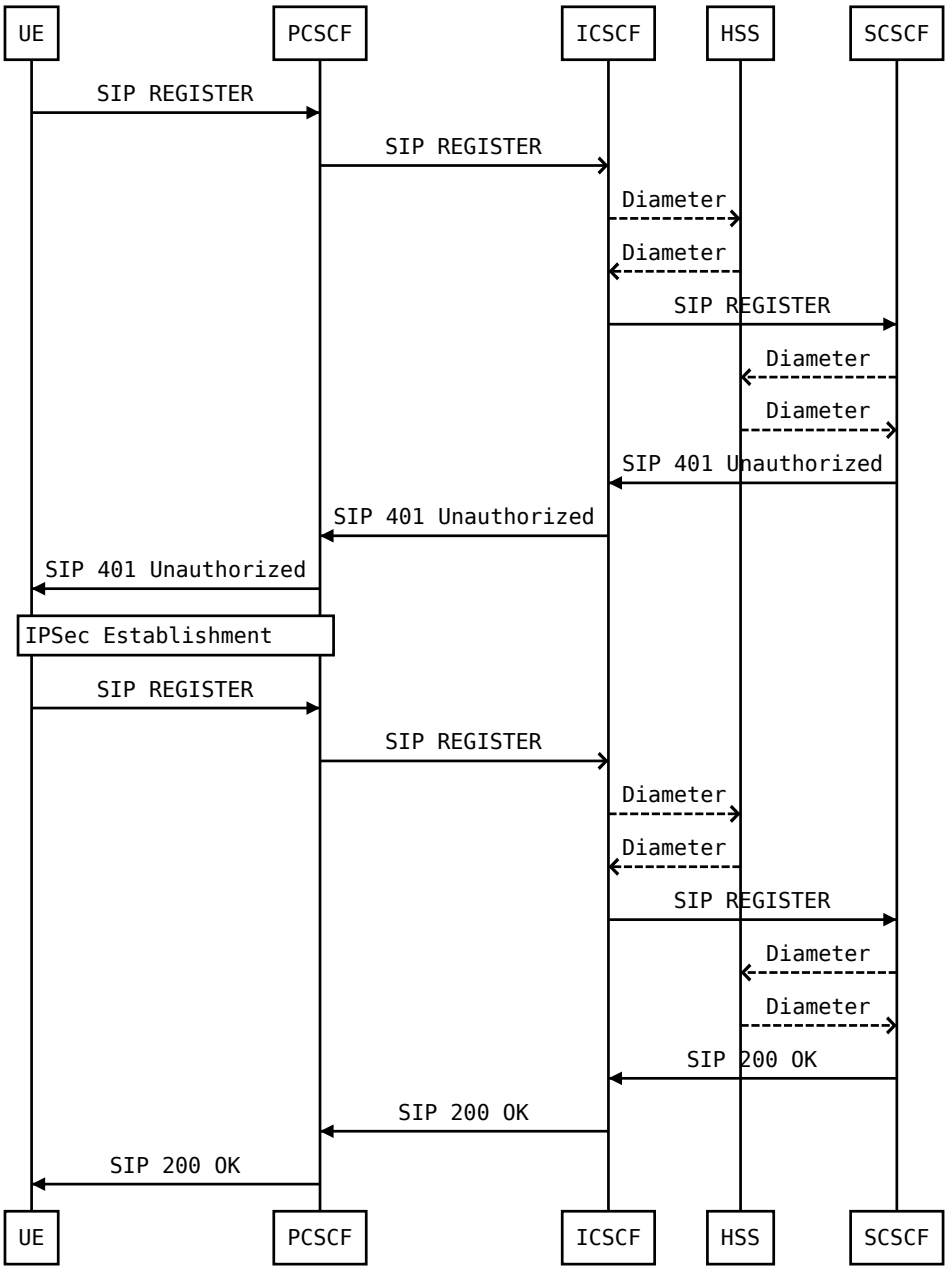

Fig. 10. VoLTE registration call-flow

The challenge is sent to the UE once the first SIP *REGISTER* message is received, then submitted to the USIM to get a RES parameter for AKA SIP answer, IK (Integrity Key) for IPsec authentication and CK (Cipher Key) for IPsec encryption.

This SIP message, and its parsing by the core network, is particularly sensitive due to the nature of the network elements that will be using the data inside the *REGISTER*. These data are not only handled by the P-CSCF but also by the I-CSCF, S-CSCF and by the most critical one: the HSS.

Depending of the network elements' (NE) configuration and SIP implementation, it is possible to perform a Denial of Service (DoS) by using flood and fuzzing techniques specific to the SIP *REGISTER* message (Listing 1). These DoS techniques can affect a large part of the IMS core network, without being registered on the P-CSCF.

An active vulnerability that allows enumeration of subscribers contained in the HSS, using the *REGISTER* method is described in Section 4.1 "IMS User enumeration using INVITE message" on page 372.

3.2 Dialing

Please note:
We will not describe all the mechanisms involved in this call-flow. For more information, please visit the following links:

- *eventhelix*[6]
- *hongjoo71 blogspot*[7]

In this part, we will analyze the different parts of the call flow between the caller UE, the IMS core network and the callee UE during a standard basic VoLTE call. Some of these exchanges, like the *INVITE* request and the *183 Session Progress* response, are involved in the vulnerabilities we present.

The initial event for VoLTE call establishment is a SIP *INVITE* request from the caller (UE-A) to the callee (UE-B). Once the different parts of the IMS network (both caller IMS network and callee IMS network) get the *INVITE* message, then forward it to the callee, who will answer with *183 Session Progress* (Figure 11).

This message is essential for the vulnerabilities presented in Section 5 "Passive vulnerabilities" on page 376 because no CDR (Charging Data

[6] `http://www.eventhelix.com/ims/ims_to_ims_call/`
[7] `http://hongjoo71-e.blogspot.fr/`

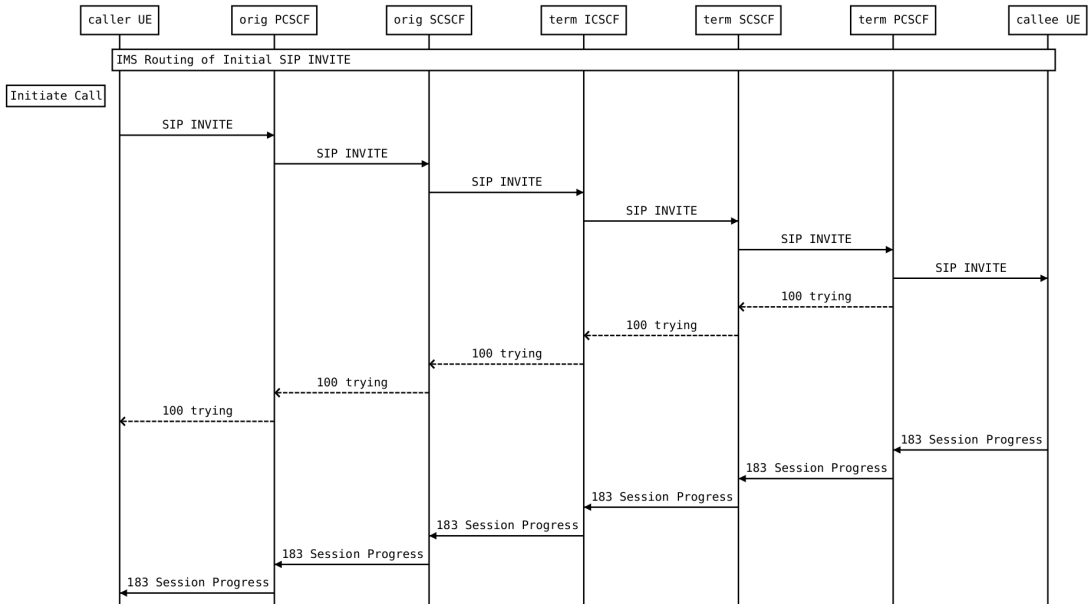

Fig. 11. First request-response during VoLTE communication

Record – billing from the operator) is generated at this point and no notification is sent to the victim (callee).

As you can see in the call flow in Figure 12, PDP context and Audio parameters are configured and exchanged after receiving the *183 Session Progress*. Concerning the messages in the call flow after PDP context activation, all of them in "normal line" (*180 RINGING* and *200 OK*) are sent to each network element, except for those in dashed lines, which are not forwarded to the callee I-CSCF.

The main purpose of this call-flow is to warn the reader that after sending only one SIP *INVITE* message to a target, we will receive a *183 Session Progress* message. It is also important to notify that the billing part is done by the network, once it receives *200 OK* from the callee (UE-B) i.e. if an attacker (caller – UE-A) interrupts the dialing call-flow after the reception of *183 Session Progress* response, no generation of Charging Data Record (CDRs) is done.

The following SIP message (Listing 2) is a typical an *INVITE* message received by a victim (UE-victim) from an attacker (UE-attacker), that will be used for vulnerabilities described in the next section (lines 5 and 13):

```
1 INVITE sip:{UE_victim_imsi}@[{UE_victim_ip}]:6000;transport=udp SIP
      /2.0
2 Call-ID: 4021427@imsgroup01.ims.operator.net
3 Via: SIP/2.0/UDP [{PCSCF_ip}]:6000;branch=
      z9hG4bK3ddf1b02ea41d1108745db149
```

```
To: <sip:+{UE_victim_msisdn}@ims.mnc042.mcc123.3gppnetwork.org;user=phone>
From: <sip:+{UE_spoofed_msisdn}@ims.mnc042.mcc123.3gppnetwork.org;user=phone>
User-Agent: {UE_attacker_User_Agent}
CSeq: 1 INVITE
Accept: application/sdp,application/3gpp-ims+xml
Allow: INVITE,BYE,REGISTER,ACK,OPTIONS,CANCEL,SUBSCRIBE,NOTIFY,PRACK,INFO,REFER,UPDATE
Contact: <sip:{PCSCF_id}@[{PCSCF_ip}]:6000;x-afi=1;encoded-parm=cGsgcmVnYXJkZXIgY2UgZ2VucmUgZGUgZGV0YWlsPwo>;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel";+g.3gpp.ps2cs-srvcc-orig-pre-alerting;+sip.instance="<urn:gsma:imei:{UE_attacker_IMEI}>";+g.3gpp.mid-call
Content-Type: application/sdp
Max-Forwards: 42
P-Asserted-Identity: <sip:+{UE_spoofed_msisdn}@ims.mnc042.mcc123.3gppnetwork.org;user=phone>
User-Agent: {UE_attacker_User_Agent}
Content-Length: 750

v=0
o= {PCSF_name} 1273402436 1273402436 IN IP6 {FQDN_ims_network}
s= --
c=IN IP6 {MGW_ip}
b=AS:38
b=RS:475
b=RR:1425
t=0 0
m=audio {RTP_port} RTP/AVP 116 96 8 18 111 110
i= AAAAAAAAAAAAAA[.....]AAAAAAAAAAAAAA
a=rtpmap:116 AMR-WB/16000/1
a=fmtp:116 mode-set=0,1,2; mode-change-capability=2; max-red=0
...
a=maxptime:240
```

Listing 2. SIP INVITE message received by callee

4 Active vulnerabilities

Attacks presented in this paper can be performed effectively and massively thanks to fingerprinting vulnerabilities that enable mass scanning of target netblocks to find vulnerable systems. Two variant vulnerabilities enable respectively to identify VoLTE subscribers (VKB#1518[8]) and RCSe-enabled subscriber (VKB#1519) by analyzing response to SIP OPTIONS messages for URN that describes VoLTE capabilities (MMtel URN) and RCSe capabilities (RCSe URNs). On top of that, there are often equipment fingerprinting vulnerabilities that enable to identify IMS

[8] VKB# ID is a unique, common identifier for Telecom specific vulnerabilities. It is used in all P1 Products.

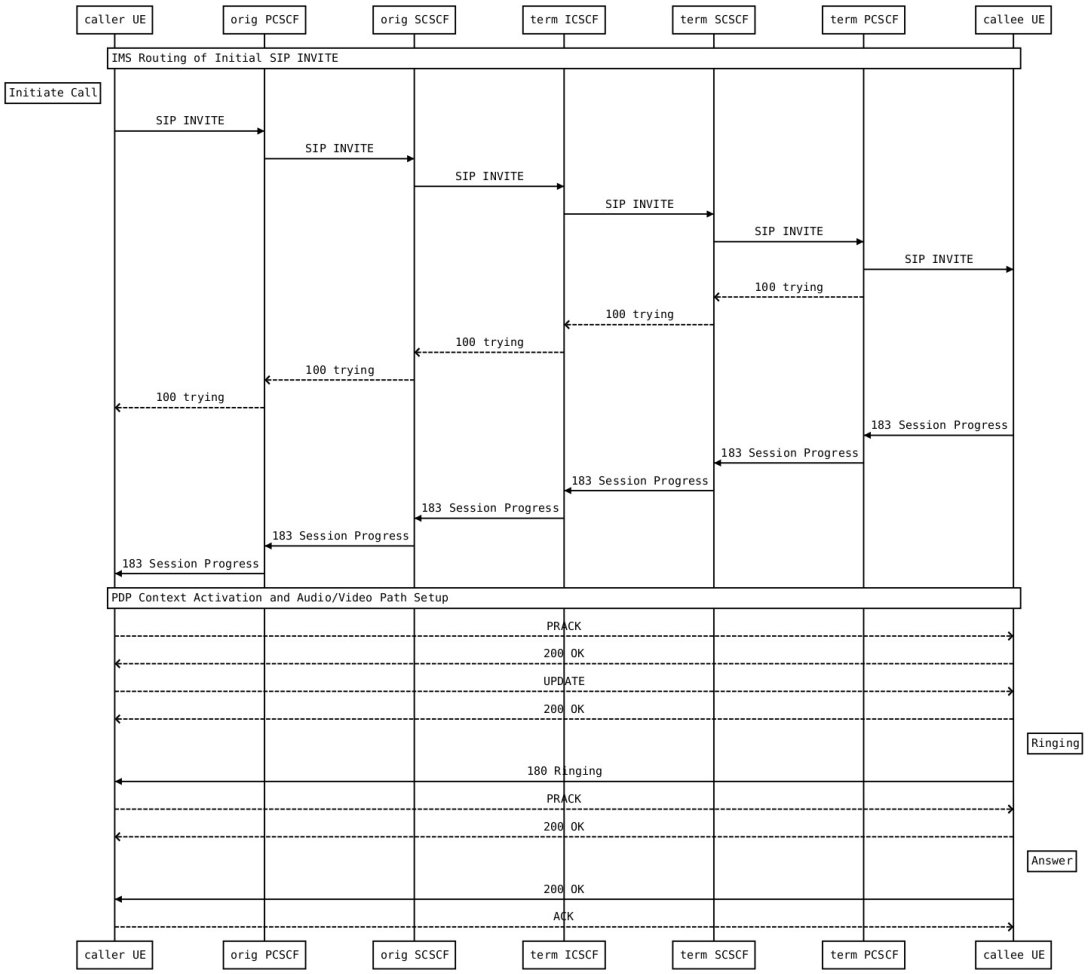

Fig. 12. Simplify call-flow for dialing in VoLTE

and VoLTE network elements in order to target specifically these network, sometimes even from the Internet public perspective.

To simplify the comprehension of the vulnerabilities presented below, we consider that the caller is the UE-attacker and the callee is the UE-victim,d i.e. the attacker is the one who sends SIP messages to the victim.

We also separate those vulnerabilities in two part: active ones and passive ones. Active vulnerabilities need particular modifications of SIP messages by the attacker and must be transmitted through the signaling bearer in order to be triggered. On the other hand, passive vulnerabilities can be detected just by sniffing the traffic on a rooted Android device.

4.1 IMS User enumeration using INVITE message

We found out that it was possible – with some core network implementations of P-CSCF – to bruteforce all the IMS users provisioned in the HSS using the INVITE message. This attack can be done directly from a subscriber's perspective by sending SIP INVITE messages over the access segment (injection directly in signaling bearer). This attack will however, imply that the attacker is already registered on the network.

Severity	Low
Title	IMS user MSISDN enumeration using *INVITE* message
VKB# ID	VKB#1409
Protocol	SIP
Type	Protocol vulnerability
Detection case	SIP *500 CX Unable To Comply response* response received, if the subscriber not exist
Impact	Disclosure of the MSISDN of IMS users
Countermeasures	Rate limit of SIP INVITE messages The P-CSCF should detect this abnormal behaviour (*INVITE* with callee number different each time) Operator should monitor the security of their SIP / IMS / VoLTE core using dedicated VoLTE-aware IDS to detect incoming attacks

When a callee victim is already provisioned in the IMS network, the network and handset will normally process SIP with Trying and Ringing (Figure 12). If the victim is not registered, the network's answer will be different: it can either be an error message or some forwarding indication. To bruteforce and enumerate, the attacker has to modify the *To* header of

the INVITE message. For each message sent, they can receive a *SIP 500 CX Unable To Comply* response if the targeted MSISDN does not exist.

4.2 Free Data channel over SDP

SDP is a text-based protocol that make parsing and sanitizing more difficult for network elements. We were able to inject arbitrary strings into SDP existing header, without triggering any operator's protection. Such attacks, if realized with specific SIP methods, can bypass the generation of CDRs (billing) and could potentially bypass Lawful Interception (LI), depending on the operator's network architecture maturity as well as the data, saved by LI network elements.

Severity	Medium
Title	Free Data channel over SDP
VKB# ID	VKB#1454
Protocol	SDP
Type	Implementation vulnerability
Detection case	Encapsulated data in SDP header sent by UE-A and receive by UE-B without being modified
Impact	P2P channel between UE's that bypass CDR's and possibly L.I
Countermeasures	Sanitizing of all SDP headers (extra fields and legitimate ones) Implement DPI (Deep Packet Inspection) in P-CSCF checking mechanism

In their academic paper [5] written in 2015, Hongil Kim and Dongkwan Kim present "Potential Free Data Channels" using SIP and RTP messages. They describe SIP/RTP tunneling attack done by encapsulating data into valid messages that will be sent to the UE-B. They further describe that it can possibly bypass the CDRs generation (billing). The following attack describes how SIP *INVITE* message are used to create a free data channel between UE-A and UE-B when using existing header in SDP part.

Also, Hendrik Schmidt and Brian Butterly from ERNW GmbH briefly discussed about this attack in there talk at AREA41 (video [8], slides [9]) in 2016 but did not confirm its feasibility or whether they encountered this vulnerability in the wild.

This vulnerability could be exploited by customized SIP/SDP clients (like .apk) that listen to the traffic on the signaling interface (*rmnet1*)

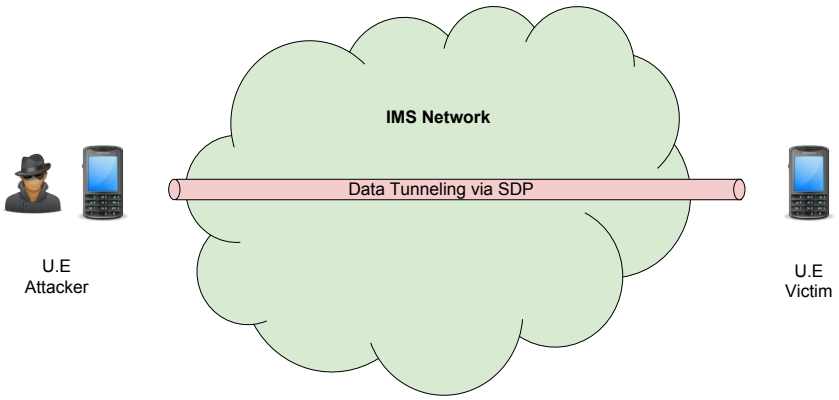

Fig. 13. Free Data Channel over SDP

and that will decode/encode custom information into the SDP part of the received message (Figure 13).

Sanitizing the SDP part of the frame is less usual than for SIP part, because the IMS core simply forwards or replaces data in the SDP part of the *INVITE* request, but does not use the data internally. The message in Listing 2 on page 369 is the one received by the UE-victim (line 26).

4.3 MSISDN spoofing through SIP INVITE message

A malicious user (UE-attacker) can customize certain header fields (*From* and *P-Preferred-Identity*) of a SIP *INVITE* request in order to trick the different network elements present on the SIP signaling path. This fake information, if left as is, not sanitized and not replaced, could be received by the target (UE-victim) and make calls appear from another (spoofed) identities (Figure 14).

Severity	Critical
Title	MSISDN spoofing through SIP *INVITE* message
VKB# ID	VKB#1455
Protocol	SIP
Type	Implementation vulnerability and/or configuration vulnerability
Detection case	UE-Attacker fake the MSISDN value of *From* and *P-Preferred-Identity* headers field in SIP *INVITE* request. UE-victim receive *From* and *P-Asserted-Identity* that contains fake phone number.
Impact	Spoofing subscriber identity
Countermeasures	Replace the two headers that contains the phone number (MSISDN) by the IMS core network

This vulnerability has been disclosed publicly by Hongil Kim and Dongkwan Kim in 2015 in their academic paper [5] and they also presented their results at CCC32 (video [3], slides [4])

In an appropriate call flow process, this may result in a UE ringing with a spoofed MSISDN displayed on the screen. As a side note, this is the exact kind of vulnerabilities that have affected Voice Mail Box security by giving password-less access to attackers. This vulnerability could also reflect a Lawful Interception problem if the LI network element base their filtering on the spoofed *From* and *P-Preferred-Identity* fields, received by the P-CSCF.

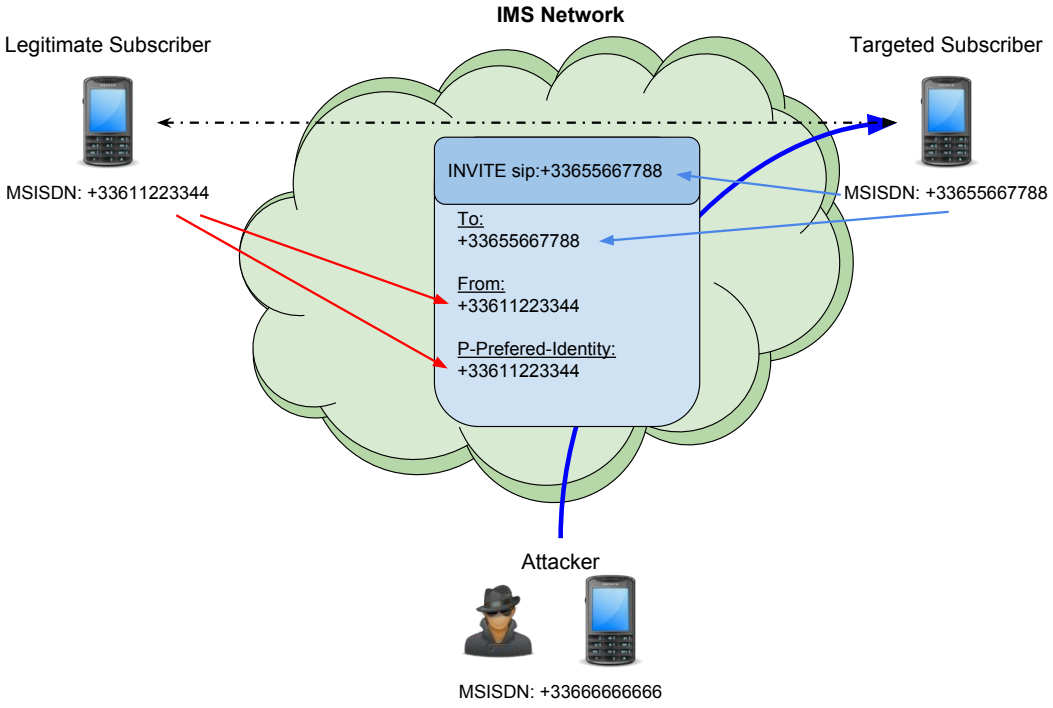

Fig. 14. MSISDN spoofing through SIP INVITE message

The *P-Asserted-Identity* field is added by the S-CSCF (Serving-Call State Control Function) to the SIP *INVITE* message, before forwarding this message to the callee (UE-victim). The *INVITE* message in Listing 2 on page 369 is the one received by the UE-victim, with the spoofed field (lines 5 and 13).

5 Passive vulnerabilities

P1 Security not only performs many audits for many different operators and their respective product/vendor mix – each specific to a Region of the World – we also get to see the other side of the fence by defending telecom and mobile networks, from the signaling IDS monitoring point of view. This enables us to gather on many missions, many vendors and many deployments a variety of vulnerabilities as well as real world attacks that have not been found, previously disclosed to the public nor shown by other researchers. The following vulnerabilities can be detected by just sniffing the incoming traffic on the signaling segment.

5.1 SIP Technical information leaked in "200 OK" messages, leads to SIP, IMS, VoLTE equipment fingerprinting and topology discovery

This vulnerability allow an attacker to fingerprint network equipment of the target operator and has been detected after receiving the *200 OK* SIP message when the UE operates the registration process to the IMS network.

Severity	Low
Title	SIP Technical information leaked in *200 OK* messages, leads to SIP, IMS, VoLTE equipment fingerprinting and topology discovery
VKB# ID	VKB#1495
Protocol	SIP
Type	Implementation vulnerability and/or configuration vulnerability
Detection case	Specific SIP header (not documented in the SIP RFC) present in SIP *200 OK* response
Impact	Fingerprinting of network elements in the operator IMS network
Countermeasures	Sanitizing these specific headers when P-CSCF forward the vulnerable *200 OK* SIP message

Some extra headers can be added by IMS network elements and lead to fingerprinting of the brand and version of the network element. With this information, an attacker can perform targeted attacks in order to DoS the operator infrastructure. For example, fingerprinting Siemens equipment is possible, thanks to the extra (non-documented) headers (Listing 3) that

are included in the SIP *200 OK* response made from the S-CSCF when the registration is done (Figure 10):

```
SIP/2.0 200 OK
...
P-com.siemens.maximum-chat-size:1300
P-com.siemens.maximum-IM-size:1300
P-com.siemens.chat:direct
...
```

Listing 3. SIP 200 OK

5.2 Leak of personal information (IMEI) about other UE subscriber (callee) in SIP "183 session Progress" message

IMEI of the callee subscriber (UE-victim) is leaked into SIP *183 Session Progress* message, received by attacker (UE-attacker) after sending the *INVITE* message (Figure 15).

Severity	Medium
Title	Leak of personal information (IMEI) about other UE subscriber (callee) in SIP *183 session Progress* message
VKB# ID	VKB#1463
Protocol	SIP
Type	Implementation vulnerability and/or configuration vulnerability
Detection case	IMEI value of the callee (UE-victim) receive in SIP *183 Session Progress* response
Impact	Leak of B-party private information
Countermeasures	Sanitizing the *Contact* header

During the writing of this paper, we discovered that ERNW GmbH mentioned something about this kind of vulnerability in one VoWiFi blog post[9] published in October 2016. However, they did not specify that it started with VoLTE and that it had been "introduced" recently in VoLTE SIP messages.

An attacker can silently get the IMEI of the callee and stop the normal call-flow of VoLTE numbering without any notification to the target (stealth mode).

[9] `https://insinuator.net/`

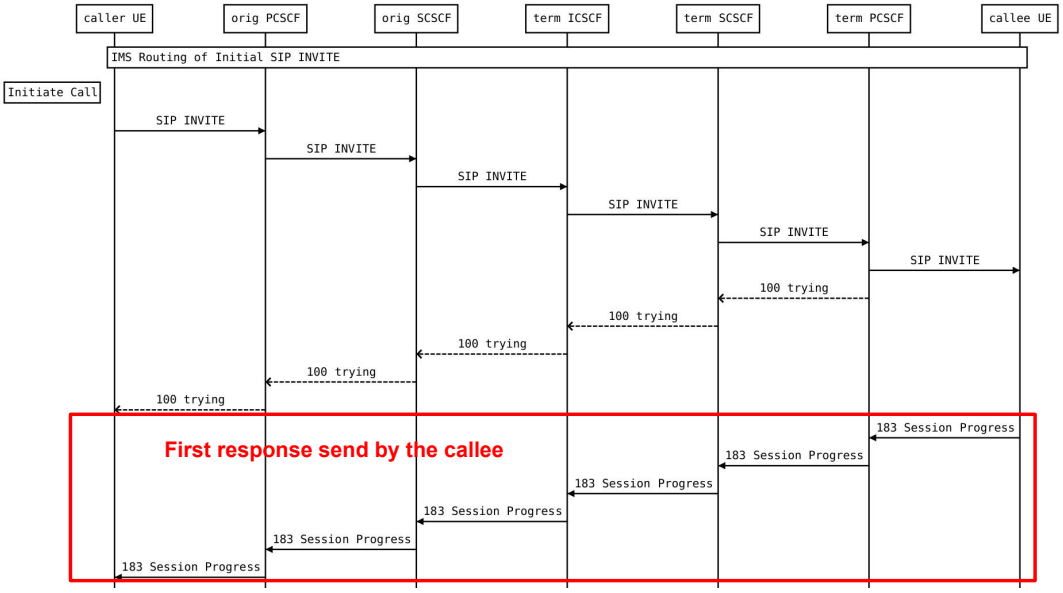

Fig. 15. SIP 183 SESSION PROGRESS received after sending initiate INVITE

As defined in the recent RFC 7255[10], "This specification defines how the Uniform Resource Name (URN) reserved for the Global System for Mobile Communications Association (GSMA) identities and its sub-namespace for the International Mobile station Equipment Identity (IMEI) can be used as an instance-id. Its purpose is to fulfill the requirements for defining how a specific URN needs to be constructed and used in the "*+sip.instance*" Contact header field parameter for outbound behavior." The IMEI value of the callee is available for an attacker in the *+sip.instance* part of the Contact header present in the SIP *183 Session Progress* response (line 6 in Listing 4).

```
1 SIP/2.0 183 Session Progress
2 Content-Length: 530
3 User-Agent: IM-client/OMA1.0 Samsung/SM-G920F-XXU2BOFJ Samsung-RCS
      /5.0
4 P-Access-Network-Info: 3GPP-E-UTRAN-FDD;
      utran-cell-id-3gpp={UE_victim_cellid}
5 Allow: INVITE,BYE,REGISTER,ACK,OPTIONS,CANCEL,SUBSCRIBE,NOTIFY,PRACK
      ,INFO,REFER,UPDATE
6 Contact: <sip:{PCSCF_id}@[{PCSCF_ip}]:6000;x-afi=1;encoded-parm=
      cGsgcmVnYXJkZXIgY2UgZ2VucmUgZGUgZGV0YWlsPwo>;+g.3gpp.icsi-ref="
      urn;urn-7;3gpp-service.ims.icsi.mmtel";
      +sip.instance="<urn:gsma:imei:{UE_victim_IMEI}>"
7 CSeq: 1 INVITE
8 Call-ID: 1920569543@{UE_attacker_ip}
```

[10] https://tools.ietf.org/html/rfc7255

```
9  Via: SIP/2.0/TCP [{UE_attacker_ip}]:6000;received={UE_attacker_ip};
       branch=cGFzIGRlIG5vbSBkJ29wZXJhdGV1ciBpY2kgO3AK;rport=5461;
       transport=TCP
10 To: <sip:+{UE_attacker_msisdn}@ims.mnc042.mcc123.3gppnetwork.org;
       user=phone>;tag=58203661
11 From: <sip:+{UE_victim_msisdn}@ims.mnc042.mcc123.3gppnetwork.org>;
       tag=824017290
12 Content-Type: application/sdp
13 RSeq: 1
14 P-Asserted-Identity: <sip:+{UE_attacker_msisdn}@ims.mnc042.mcc123.3
       gppnetwork.org;user=phone>
15 Server: {PCSCF_User_Agent}
16
17 [SDP]
18 ...
19 [/SDP]
```

Listing 4. SIP 183 Session Progress response

5.3 Leak of personal information ("*utran-cell-id*") about other UE subscriber (callee) in SIP "183 Session Progress" message

We found that it was possible to remotely localize and track other VoLTE subscribers, by sending only one request (SIP *INVITE*) and use the information contained in the victim's response (SIP *183 Session Progress* message).

Severity	Critical
Title	Leak of personal information (utran-cell-id) about other UE subscriber (callee) in SIP *183 Session Progress* message
VKB# ID	VKB#1468
Protocol	SIP
Type	Implementation vulnerability and/or configuration vulnerability
Detection case	*utran-cell-id-3gpp* value of UE-victim received in SIP *183 Session Progress* response
Impact	Leak of B-party private information – geolocation
Countermeasures	Replacing/removing *P-Access-Network-Info* header by the IMS core network

A Similar geolocation of callee subscriber are mentioned by Seongmin Park and Sekwon Kim in their paper [7]. The authors found out that the CellID value (unique identifier of a physical antenna) is present in the

SIP *200 OK* message retrieved by the victim. This message is received by the attacker after a lot of SIP exchanges were involved. The following vulnerability is more silent (no ringing) and free of charges (no CDRs).

The interesting "*utran-cell-id-3gpp*" value is contained in *P-Access-Network-Info* header (line 4 in Listing 4 on page 378). The "*utran-cell-id-3gpp*" value is composed of 4 information (Figure 16):

- MCC: Mobile Country Code. This code identifies the country (e.g. : France - 208)
- MNC: Mobile Network Code. This code identifies the mobile operator. (e.g. : Free - 15).
- LAC: Location Area Code is a unique number corresponding to the current location area. A location area is a set of base stations that are grouped together to optimize signaling.
- UTRAN CellID (LCID): Concatenation of the RNC-ID (ID of the Radio Network Controller) and the Cell ID (ID of the cell – CID).

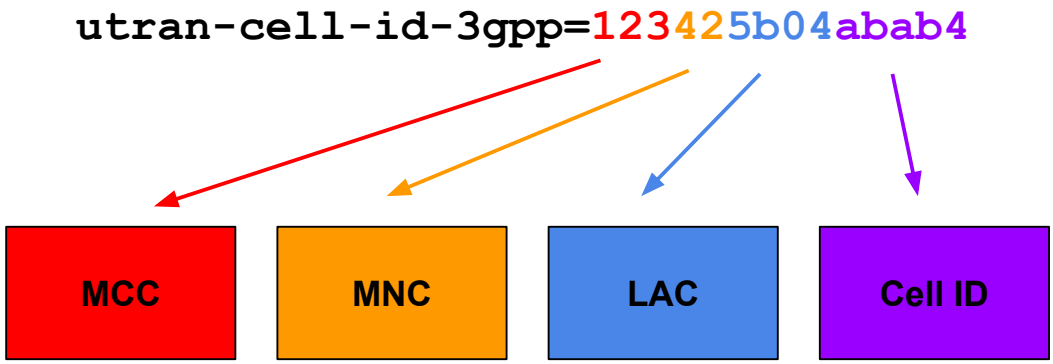

Fig. 16. UTRAN CellID decomposition

Once an attacker gets this information about his target (UE-victim), he can easily retrieve the victim's localisation using databases of Cell IDs like OpenCellID[11] / Cell ID Finder[12]. or using public Geolocation API like Alexander Mylnikov's website[13].

[11] `https://opencellid.org/`
[12] `http://cellidfinder.com/`
[13] `https://www.mylnikov.org/archives/1059`

6 Conclusion

VoLTE is intentionally not a complex technology. The different IP protocols used make it easier to understand for non-telecom experts, than other telecom protocol stacks. Also, VoIP heritage and text-based SIP protocol create new attack surfaces that make the operator network accessible and exposed more easily, than in legacy networks (as demonstrated, a VoLTE SIM card and a rooted Android smartphone are sufficient to perform these attacks).

Bad default vendor configuration in some network elements and/or misconfiguration during network elements' deployment may very well result in having these vulnerabilities still present in some operators' networks.

P1 Security hopes that this paper and the related talk are going to help operators and vendors better understand these risks and efficiently counter the low complexity attacks they will be facing in the years to come.

References

1. GSM Association. Volte service description and implementation guidelines. `http://www.gsma.com/network2020/wp-content/uploads/2014/05/FCM.01-v1.1.pdf`, 2014.
2. GSA. Volte service description and implementation guidelines. `http://www.voiceage.com/pdfs/170131-SNAPSHOT-VoLTE_January_2017.pdf`, 2017.
3. Hongil Kim and Dongkwan Kim. Dissecting volte. `https://media.ccc.de/v/32c3-7502-dissecting_volte`, 2015.
4. Hongil Kim and Dongkwan Kim. Dissecting volte. `https://lab.dsst.io/32c3-slides/7502.html`, 2015.
5. Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim. Breaking and fixing volte: Exploiting hidden data channels and mis-implementations. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, pages 328–339, New York, NY, USA, 2015. ACM.
6. Benoit Michau and Christophe Devine. How to not break lte crypto. `https://www.sstic.org/media/SSTIC2016/SSTIC-actes/how_to_not_break_lte_crypto/SSTIC2016-Article-how_to_not_break_lte_crypto-michau_devine.pdf`, 2016.
7. Seongmin Park, Sekwon Kim, Kyungho Son, and Hwankuk Kim. Security threats and countermeasure frame using a session control mechanism on volte. In *Proceedings of the 2015 10th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)*, BWCCA '15, pages 532–537, Washington, DC, USA, 2015. IEEE Computer Society.
8. Hendrik Schmidt and Brian Butterly. Imsecure – attacking volte (and other stuff). `https://www.youtube.com/watch?v=P1u2T_TELqY`, 2016.
9. Hendrik Schmidt and Brian Butterly. Imsecure – attacking volte (and other stuff). `http://area41.io/downloads/slides/area41_16_ERNW_IMSecure.pdf`, 2016.