



SecurityGen

Telecom Security. Transcending Generations.

VOLTE

A history of disregard

Table of contents

- 3** Executive summary
- 3** History of VoLTE
- 4** Voice evolution in mobile networks
- 5** Security oversights and their consequences
- 6** Attack vector: VoLTE subscriber
 - IP connectivity
 - Nmap scan
 - Direct connection to other phones
 - Lack of encryption
- 13** SIP protocol issues
 - Information disclosure in messages sent to the subscriber
 - Incorrect anonymous call implementation
 - Lack of SIP Flood protections
 - No sanitation of experimental headers
 - Impersonated SMS
- 22** Recommendations for enhancing VoLTE security
- 23** Future-proofing VoLTE / VoNR security
- 24** Terms and abbreviations
- 25** References

Executive summary

This research article delves into the evolution, current state, and future considerations regarding Voice over LTE (VoLTE) security. VoLTE, a fundamental component of modern telecommunications, facilitates the transmission of voice calls as data packets across LTE networks. Despite its advancements, VoLTE has been marred by security challenges, a result of both historical oversight and rapid technological developments.

This paper outlines the inherent technical vulnerabilities within VoLTE, illustrating real-world attack scenarios and highlighting the pressing need for telecom operators to implement their defenses. Additionally, the article provides a set of actionable recommendations aimed at mitigating these vulnerabilities. Furthermore, the article casts a futuristic outlook, examining the implications of these security measures as networks transition to 5G and beyond, emphasizing the necessity for ongoing vigilance and adaptation in the face of evolving threats.

01. History of VoLTE

IP telephony, commonly referred to as VoIP, is now widely used. The first VoIP implementation was introduced in 1995, and by the early 2000s, it began to spread rapidly. By 2003, about 25% of voice calls were made using VoIP.

Over the years, this technology has matured considerably in terms of security, largely due to the significant interest from hackers'. Protective measures against malefactors posing as subscribers are developed and well known.

VoIP concepts were integrated into the mobile network architecture in form of IMS subsystem which was chosen by 3GPP to be used as the sole option for voice calls in LTE under the name Voice over LTE (VoLTE)

The same technology is used in 5G, where it is referred to as Voice over NR (VoNR). To protect these technologies, GSMA created several documents (see FS.38 [1] and FS.22 [2]) meant to categorize known threats and adapt known protective measures.

02. Voice evolution in mobile networks

Let's observe how the changes that we discussed affect mobile network architecture. In 2G and 3G networks, there is a specific subsystem used for voice calls, which is a part of control plane segment (CS-MGW) connected to the Public Switched Telephone Network (PSTN)

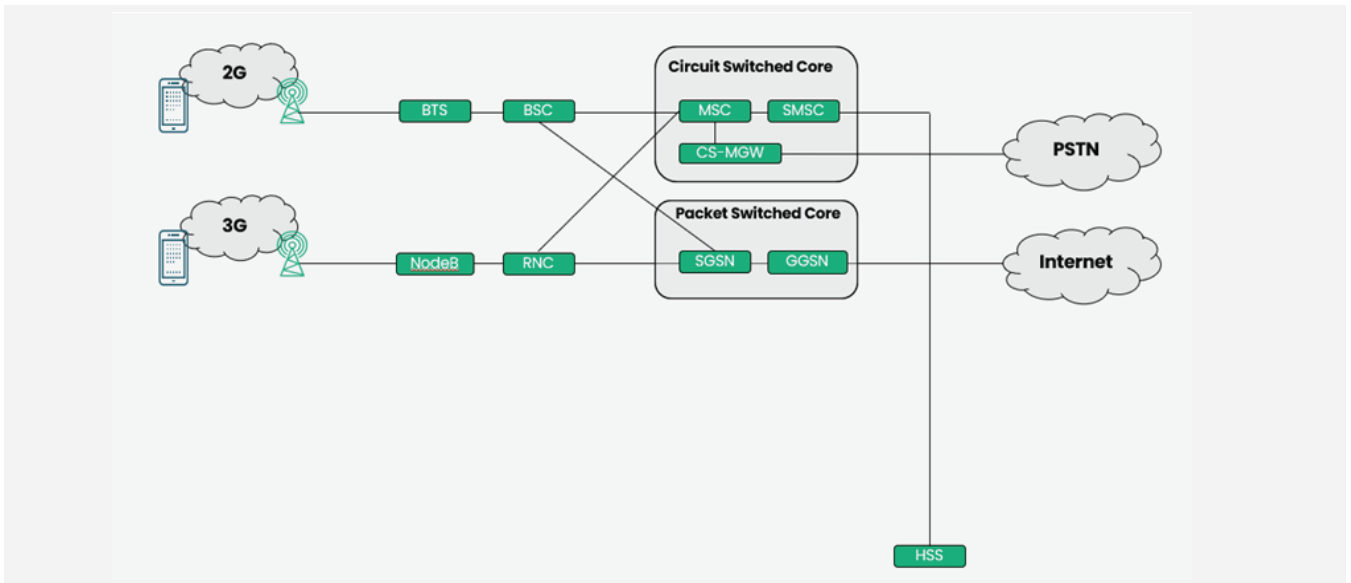


Figure 1. 2G and 3G telephony

4G network was made IP oriented, so voice subsystem was made over IP connectivity via additional IP Multimedia Subsystem – IMS.

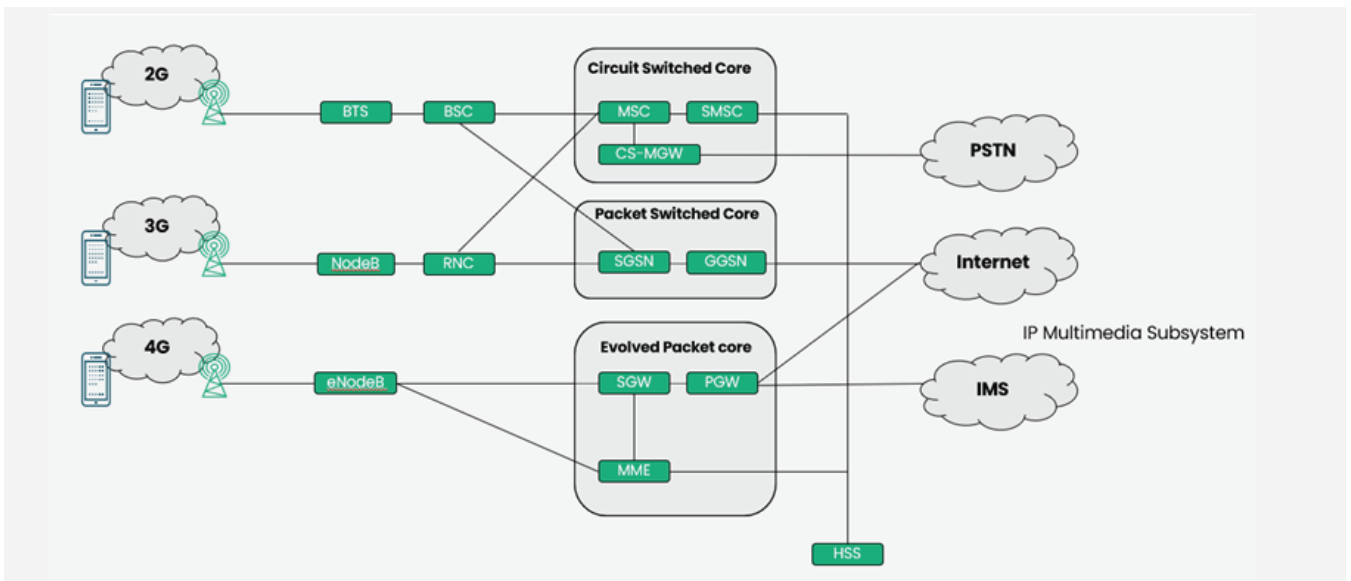


Figure 2. Place of IMS in mobile network

To deploy LTE networks quickly, a temporary solution was devised to avoid implementing IMS altogether. Initially, LTE deployments were focused on significantly increasing mobile data capabilities, with voice services not being a priority since they were adequately covered by 2G and 3G. This temporary solution switches subscribers to the 2G or 3G network when an incoming or outgoing call is initiated, promptly returning them to 4G once the call is finished to restore fast data connection. This solution is called **CS-Fallback**.

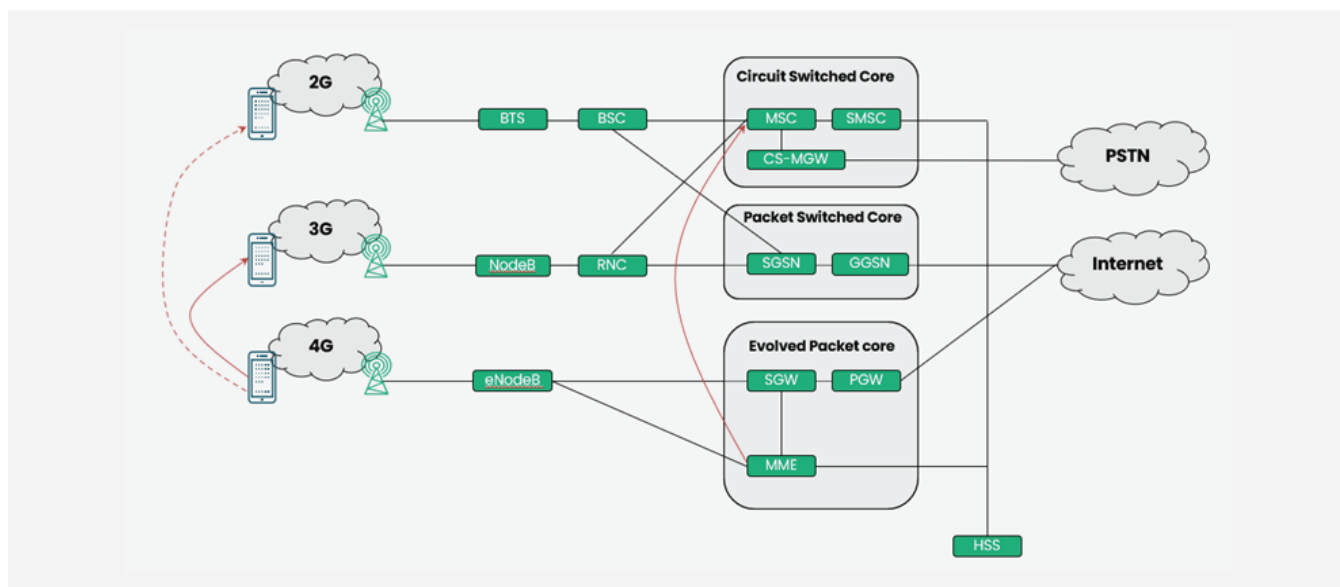


Figure 3. Voice call via CS-fallback

03. Security oversights and their consequences

The CS-Fallback implementation killed interest amongst MNOs to deploy fully operational IMS core and implement native LTE calls (VoLTE calls). Let's look at some historical data:

- The 1st LTE network was deployed in December 2009 by TeliaSonera in Sweden and Norway.
- The 1st VoLTE network support was introduced in August 2012 in USA, along with the 1st mobile phone which was capable to use it – LG Connect 4G.
- A full-featured VoLTE network was deployed in May 2014 in Singapore, although the only capable phone in this case was Samsung Galaxy Note 3.
- Only in 2020 it became commonplace for almost all new phones to have VoLTE support.

It took more than 10 years to make the industry ready for VoLTE, as it's not possible to switch off 2G and 3G networks until all phones support VoLTE. Due to the slow

progress of industry, not many operators were interested in deploying VoLTE. The only driving force behind it is the desire to phase out legacy 2G and 3G networks and use their frequency spectrum for modern technologies like 4G and 5G.

Several operators around the world implemented this, but it only became a significant issue in December of 2022 with USA Verizon shutting down their 2G and 3G networks. It was a small step for one operator, but a significant one for the industry, as other MNOs realized that their subscribers couldn't use voice services while on roaming in the USA. It turned into a race for VoLTE deployment in 2023. Some operators implemented it in a few months. And you can easily guess, security was not a priority for such VoLTE deployments. While security controls are implemented in the form of SIP proxies, we found that there are several things specific for mobile operators that may be overlooked.

04. Attack vector: VoLTE subscriber

Currently, almost any MNO in the world provides VoLTE in some capacity. As it was presented at [3], to access IMS network in a way of usual data connectivity you only need to add IMS APN in your phone and change APN type to the "default".

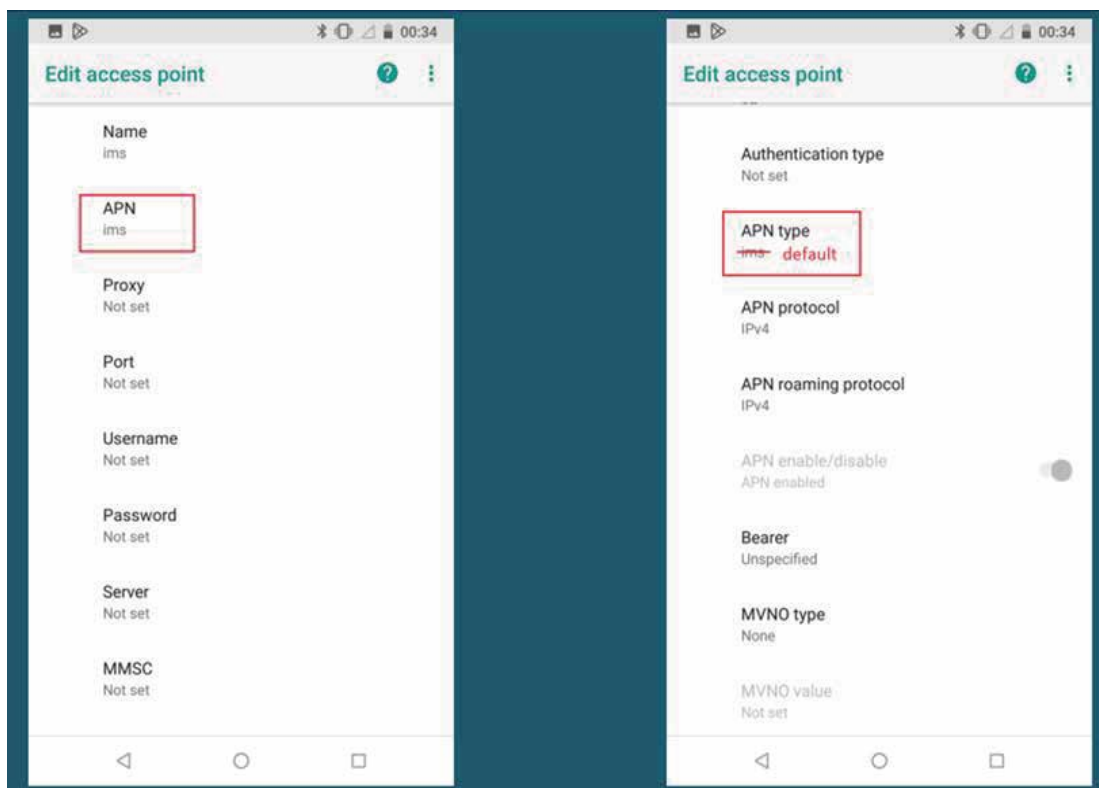


Figure 4. Using IMS APN for usual data connection to access IMS core

But it may be not convenient to use phone for testing, so it is possible to connect usual laptop via 4G-dongle using IMS APN instead of using default "internet" APN.

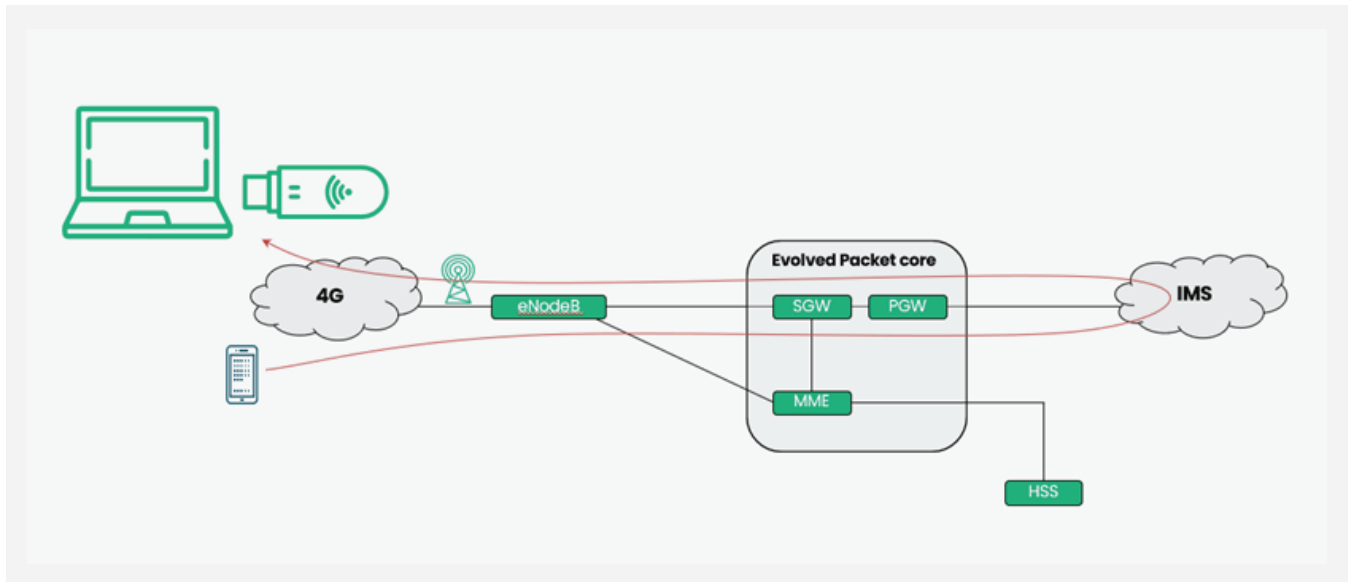


Figure 5. Using laptop for IMS connectivity

Picture below shows the IMS infrastructure you may reach once connected.

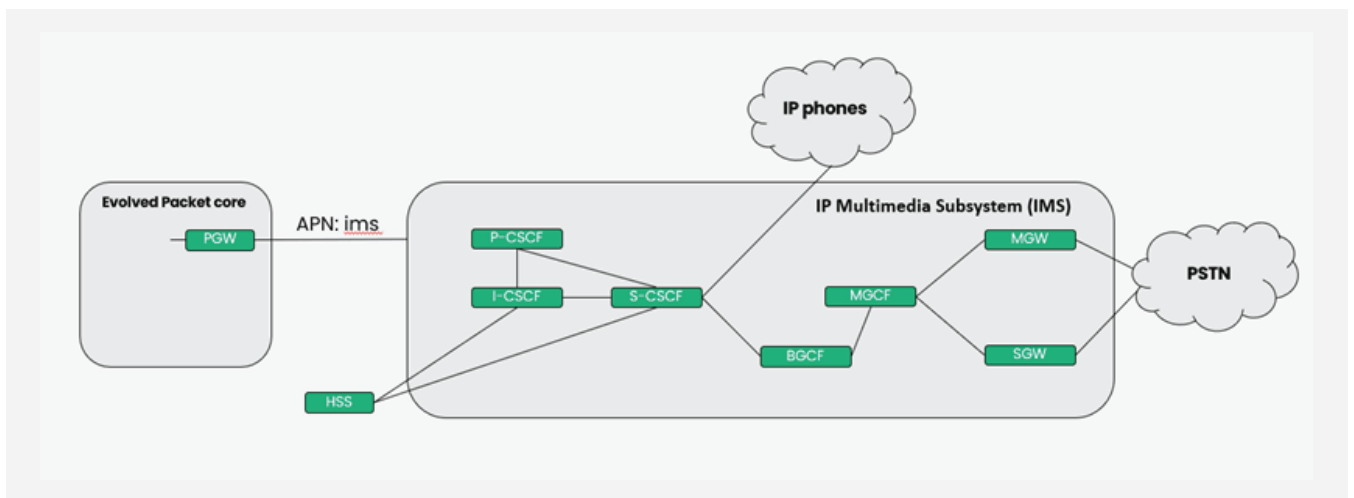


Figure 6. IMS structure

So, let's see what happens when we try to apply threats described in [1] and [2] to a real network.


```
#####
# ATTENTION: AUTHORIZED PERSONAL ONLY. DISCONNECT IMMEDIATELY #
#####
User Authentication
Enter password:
User Authentication
Enter password:

sguser@ims:~$ ssh admin@10.129.129.129

#####
# ATTENTION: AUTHORIZED PERSONAL ONLY. DISCONNECT IMMEDIATELY #
#####
User Authentication
Enter password:
The user has been locked and you cannot log on it.
User Authentication
Enter password:
```

Figure 9: Locking the password for admin user via SSH

This could enable malefactor to gain control of the attacked nodes. Allowing them to alter the configuration to perform fraudulent activities. Even if the hack isn't successful, DDoS attacks on the unhardened nodes should still be feasible.

Administrator accounts may also be locked on the nodes in the core

network. It is crucial to note, that hacking of these nodes is more concerning than in traditional VoIP cases because compromised MNO nodes may provide malefactor an access to the signaling networks. Usually, MNOs serve a lot of subscribers and are interconnected, thus making signaling attacks much more dangerous.

Blocking SSH from the user side is common sense, so the lack of this demonstrates a disregard for security from this attack vector.

4.1.2. Direct connection to other phones

We also see that the same IP connectivity allows direct IP access to other phones. As data on VoLTE bearer is usually not charged (calls are), malefactor may setup direct connectivity services to avoid any charging. This largely depends on the network implementation and occurs due to the lack of segmentation between subscribers connected to the same P-CSCF.

Malefactors may exchange large files or, using a PC with USB dongle, set up free internet access for other phones in the same IP subnet.

This usually works for all subscribers connected to the operator's network, meaning that this subscriber may be roaming in another country and still use this free internet service.

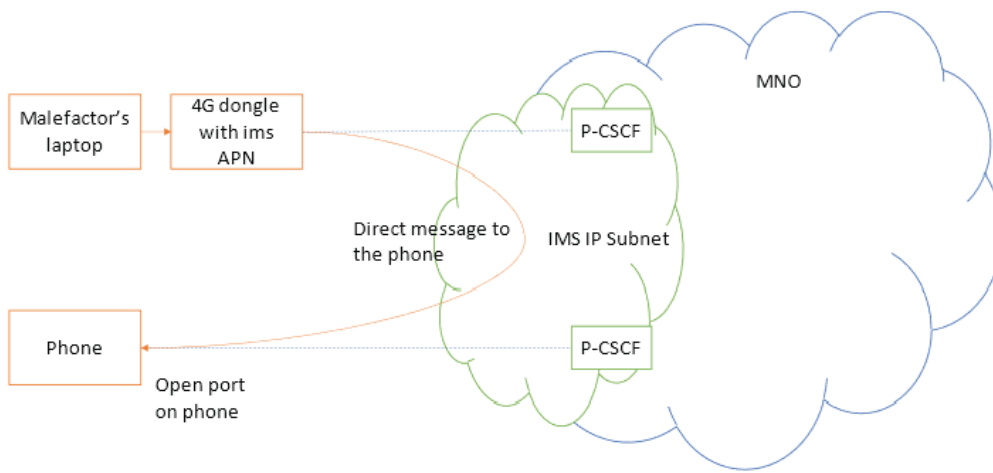


Figure 10: direct messaging attack scheme

```

sguser@ims:~$ ping b:87cc
PING b:87cc (b:87cc) 56 data bytes:
64 bytes from b:87cc: icmp_seq=1 ttl=62 time=918 ms
64 bytes from b:87cc: icmp_seq=2 ttl=62 time=51.2 ms
64 bytes from b:87cc: icmp_seq=3 ttl=62 time=60.7 ms
^C
--- b:87cc ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 51.221/343.325/918.077/406.428 ms
sguser@ims:~$ echo -n "Direct connection between handsets" | nc -w1 ab:87cc 7777
sguser@ims:~$
  
```

Figure 11: Direct communication with a phone, laptop side

```

1:27 PM 4.5G 100%
:/ # ip a show dev rmnet_data3
19: rmnet_data3@rmnet_ipa0: <UP,LOWER_UP> mtu 1500 qdisc mq state UNKNOWN group default qlen 1000
    link/[519]
    inet6 [redacted] f:feab:87cc/64 scope
    ope global dynamic mngtmpaddr
        valid_lft forever preferred_lft forever
    inet6 [redacted] ab:87cc/64 scope link
        valid_lft forever preferred_lft forever
:/ # nc -l -6 -s [redacted] f:feab:87cc
Direct connection between handsets: / #
  
```

Figure 12: Direct communication with a phone, phone side

If direct communication is possible, it may also be possible to spoof source IP addresses when targeting the phone. This may allow malefactors to impersonate traffic from network core.

1 0.0000000		ed:6692:10be	ff:fe6f:54b8	ICMP	118 Echo (ping) request id=0x0011, seq=1, hop limit=64 (reply in 3)
2 1.0262925		ed:6692:10be	ff:fe6f:54b8	ICMP	118 Echo (ping) request id=0x0011, seq=2, hop limit=64 (reply in 4)
3 1.5341772		ff:fe6f:54b8	ed:6692:10be	ICMP	118 Echo (ping) reply id=0x0011, seq=1, hop limit=57 (request in 1)
4 1.5395436		ff:fe6f:54b8	ed:6692:10be	ICMP	118 Echo (ping) reply id=0x0011, seq=2, hop limit=57 (request in 2)
5 2.0269998		ed:6692:10be	ff:fe6f:54b8	ICMP	118 Echo (ping) request id=0x0011, seq=3, hop limit=64 (request in 6)
6 2.1031481		ed:6692:10be	ff:fe6f:54b8	ICMP	118 Echo (ping) reply id=0x0011, seq=3, hop limit=57 (request in 5)
7 685.05221		ed:dead:beef	ff:fe6f:54b8	ICMP	81 Echo (ping) request id=0x08ae, seq=3333, hop limit=64 (no response found)

Figure 13. Ping with spoofed IP sent from PC.

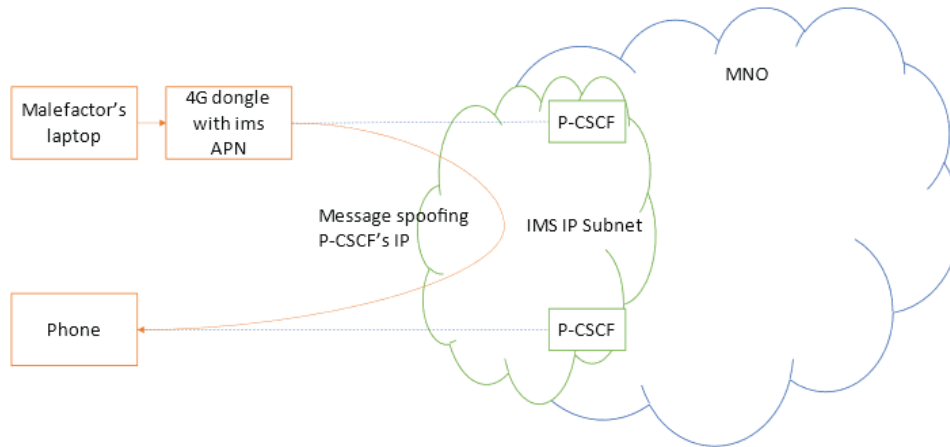


Figure 14: ip spoofing scheme

11 51.284709		ed:6692:10be	ff:fe6f:54b8	ICMP	120 Echo (ping) request id=0x0011, seq=3, hop limit=57 (reply in 12)
12 51.285077		ff:fe6f:54b8	ed:6692:10be	ICMP	120 Echo (ping) reply id=0x0011, seq=3, hop limit=64 (request in 11)
13 734.393439		ed:dead:beef	ff:fe6f:54b8	ICMP	83 Echo (ping) request id=0x08ae, seq=3333, hop limit=57 (reply in 14)
14 734.393812		ff:fe6f:54b8	ed:dead:beef	ICMP	83 Echo (ping) reply id=0x08ae, seq=3333, hop limit=64 (request in 13)
15 737.504212		a:5357	ff:fe6f:54b8	ICMP	131 Destination Unreachable (Address unreachable)

Figure 15. Ping with spoofed IP is delivered.

Note that some of the tested operators were not vulnerable. This suggests that setting up isolated subnets for subscribers is possible. Still, it appears that a lot of MNOs do not prioritise implementing this policy. **This vulnerability was first reported in [4] in 2015.**

4.1.3. Lack of encryption

Connected to this issue is the next one. A lot of networks are not using encryption. Even in cases where IPsec is used, it is often possible to negotiate “null” as encryption algorithm. This results in messages being packed in Encapsulated Security Payload, but no actual encryption occurs. E.g., you can easily set up Wireshark to show decoded packets.

If one of the network nodes is compromised and malefactor can view the subscriber’s traffic, this leads to disclosure of private information.

Unencrypted signaling traffic allows for disclosure of private information and location tracking. Unencrypted user traffic, namely, calls in RTP, leads to eavesdropping.

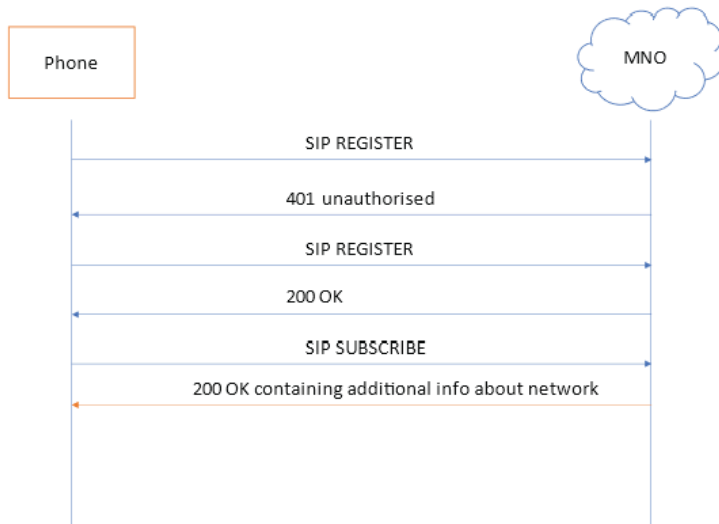


Figure 16. SIP REGISTER without IPSec scheme

Protocol	Length	alg	Info
SIP	1337	null	Request: REGISTER sip:ims.mnc[redacted].mcc[redacted].3gppnetwork.org ...
SIP	801	null	Status: 401 Unauthorized
IPv6	1014		IPv6 fragment (off=0 more=y ident=0x53771357 nxt=50)
SIP	626	null, null	Request: REGISTER sip:ims.mnc[redacted].mcc[redacted].3gppnetwork.org ...
SIP	1170		Status: 200 OK (1 binding)

Figure 17. IMS registration without encryption

Protocol	Length	Encapsulating Security Payload	CSeq	Expires	Info
SIP	668		1		OPTIONS Request: OPTIONS sip:[redacted]@ims
SIP	644		1		OPTIONS Status: 200 OK
SIP	1337		1	600000	REGISTER Request: REGISTER sip:ims.mnc[redacted]
SIP	801		1		REGISTER Status: 401 Unauthorized
SIP	626	✓	2	600000	REGISTER Request: REGISTER sip:ims.mnc[redacted]
SIP	1170	✓	2		REGISTER Status: 200 OK (1 binding)
ICMPv6	1218	✓	2		REGISTER Parameter Problem (unrecognized Next H
SIP	618	✓	3	0	REGISTER Request: REGISTER sip:ims.mnc[redacted]
SIP	1106	✓	3		REGISTER Status: 200 OK (removed 1 binding)
ICMPv6	1154	✓	3		REGISTER Parameter Problem (unrecognized Next H
SIP	668		1		OPTIONS Request: OPTIONS sip:[redacted]@ims
SIP	644		1		OPTIONS Status: 200 OK

Figure 18. Successful answers without IPSec

GSMA mandates the use of encryption for SIP signaling. However, a lot of MNOs disregard this, presumably to avoid problems with compatibility issues.

4.2 SIP protocol issues

Next, let's go one layer up and switch from lapses in IP security to the problems stemming from the incorrect configuration of SIP security controls.

4.2.1. Information disclosure in messages sent to the subscriber

Most networks will send messages with internal identifiers of network FQDNs in SIP messages.

In many cases networks that we tested seemed to disregard subscriber privacy in several different ways. Usual security lapses allow malefactors to obtain IMEI, phone model and location. See some of the examples on the screenshots below.

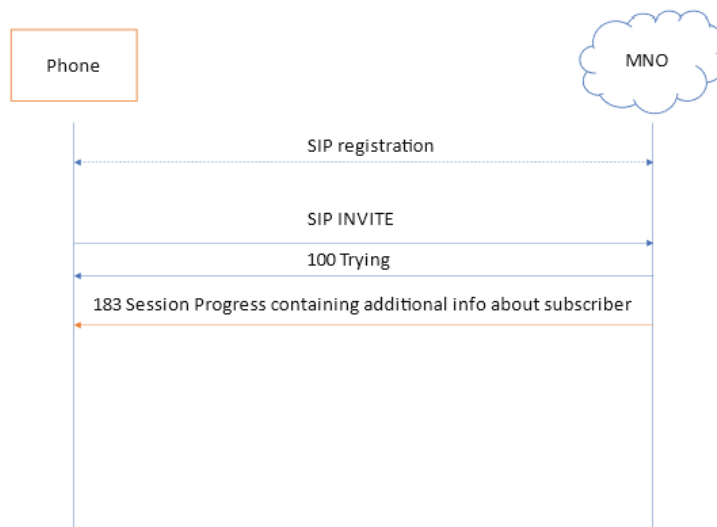


Figure 19. Disclosure of UE model scheme

In numerous cases, malefactor can gather a lot of information simply by analyzing usual messages from operator during different standard procedures like registration, calls or SMS.

For example, Figure 20 shows disclosure of a phone model and firmware version of the callee via Server field in 183 Session progress response which we received when establishing a call.

```

3 0.103428398 SIP 390 Status: 100 Trying
4 1.791051946 SIP/SDP 1400 Status: 183 Session Progress

Encapsulating Security Payload
User Datagram Protocol, Src Port: 9950, Dst Port: 7200
Session Initiation Protocol (183)
  Status-Line: SIP/2.0 183 Session Progress
  Message-Header
    Via: SIP/2.0/UDP [redacted]:7200;branch=z9hG4bK-ZLqLmZA77nrblTSQdx0goB7MHbMCF70L
    Record-Route: <sip:[redacted]:9900;lr:Hpt=nmw_276_6504196c_18079c9d_ex_9032_116;CxtId=3;TRC=ffffffff-ffffffff;X-HbB2bUaCookie=19477>
    Call-ID: jolly6[redacted]
    [Generated Call-ID: jolly6[redacted]]
    From: <sip:[redacted]@ims.mnc[redacted].mcc[redacted].3gppnetwork.org>;tag=jbcvxniE
    To: <tel:[redacted];tag=t0a426t4;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org>
    CSeq: 1 INVITE
    Allow: INVITE,ACK,CANCEL,BYE,UPDATE,PRACK,MESSAGE,REFER,NOTIFY,INFO,OPTIONS
    Contact: <sip:[redacted]:9900;Hpt=nmw_276_6504196c_18079c9d_ex_9032_16;CxtId=3;TRC=ffffffff-ffffffff>;g.3gpp.icsi-ref="urn:3Aurn-7X3A3gpp-service.ims.icsi.mmtel"
    Require: 100rel
    Server: Xiaomi/2208121200_Qualcomm_V13.0.11.0.SLFEUXM_Android12
    HSeq: 1
    P-Early-Media: gated
    P-Asserted-Service-Info: vrbt=90
    Feature-Caps: *;+g.3gpp.srvcc
    Recv-Info: g.3gpp.state-and-event-info
    Content-Length: 350
    Content-Type: application/sdp
  ----- Body

```

Figure 20. Disclosure of UE model

Another message potentially disclosing information about other subscribers is incoming SIP invite, see Figure 21 below.

```

Protocol Length Info
SIP 1512 Request INVITE sip:[redacted]@[redacted]:7400 SIP/2.0

Frame 2: 1512 bytes on wire (12096 bits), 1512 bytes captured (12096 bits) on interface unknown, id 0
Linux cooked capture v1
Internet Protocol Version 6, Src: [redacted]:06:11 Dst: [redacted]:0a:3ec3
Encapsulating Security Payload
User Datagram Protocol, Src Port: 9950, Dst Port: 7400
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:[redacted]@[redacted]:7400 SIP/2.0
  Method: INVITE
  Request-URI: sip:[redacted]@[redacted]:7400
  [Resent Packet: False]
  Message-Header
    Via: SIP/2.0/UDP [redacted]:90:0001;9900;branch=z9hG4bKt088bmc0fbtblue51ld
    Record-Route: <sip:[redacted]:90:0001;9900;lr:Hpt=90c2_16;CxtId=4;TRC=fff
    Call-ID: sbcthlNQ#t#HttlBqtubFGiuLLFtGillGbbqS1FMB@[redacted]
    [Generated Call-ID: sbcthlNQ#t#HttlBqtubFGiuLLFtGillGbbqS1FMB@[redacted]]
    From: <tel:[redacted];noa=international;srvattri=national;tag=GiiFIFMu
    To: <sip:[redacted]@ims.mnc[redacted].mcc[redacted].3gppnetwork.org>
    CSeq: 1 INVITE
    Accept: application/sdp,application/3gpp-ims+xml,application/vnd.3gpp.state-and-event-info+xml
    Allow: INVITE,ACK,OPTIONS,CANCEL,BYE,UPDATE,INFO,REFER,NOTIFY,MESSAGE,PRACK
    Contact: <sip:[redacted]:90:0001;9900;Dpt=ed6a-200;Hpt=90c2_16;CxtId=4;TR
    Max-Forwards: 62
    Supported: timer,tdialog,100rel
    User-Agent: SM-A217F-UA2 Samsung IMS 6.0
    Session-Expires: 1800
    Min-SE: 600
    P-Asserted-Identity: <tel:[redacted];noa=international;srvattri=national>
    P-Called-Party-ID: <sip:[redacted]@ims.mnc[redacted].mcc[redacted].3gppnetwork.org>
    P-Early-Media: supported
    P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
    P-Enable: 1
    Feature-Caps: *;+g.3gpp.srvcc;+g.3gpp.srvcc-alerting
    Recv-Info: g.3gpp.state-and-event-info
    Accept-Contact: *;explicit;require;+g.3gpp.icsi-ref="urn:3Aurn-7X3A3gpp-service.ims.icsi.mmtel"
    Reject-Contact: *;+g.3gpp.ics="server"
    Content-Length: 821
    Content-Type: application/sdp
  Message Body

```

Figure 21. Subscriber user-agent disclosure

Figure 22 shows S-CSCF DNS name in P-Asserted-Identity header of 200 OK response on SIP SUBSCRIBE commonly sent after initial registration.

```

32 416.6601 [redacted] SIP 1230 Request: SUBSCRIBE
33 416.9455 [redacted] SIP 1116 Status: 200 OK
35 417.0852 [redacted] SIP/XHL 990 Request: NOTIFY sip

Encapsulating Security Payload
User Datagram Protocol, Src Port: 9950, Dst Port: 7200
Session Initiation Protocol (200)
Status-Line: SIP/2.0 200 OK
Message Header
Via: SIP/2.0/UDP [redacted]:7200;branch=z9hG4bK-Q93PZcIkvZ9466Ia0WZkE8YSwbt4w0Qu;port=6200;transport=UDP
Record-Route: < sip:[redacted]:9900;lr;hpt=nm_1c8_64e72b96_1686af34_ex_8fa2_116;ctxid=3;TRC=ffffffff-ffffffff>
Call-ID: xdgZnFBF[redacted]
[Generated Call-ID: xdgZnFBF[redacted]]
From: < sip:[redacted]@ims.mnc.mcc.3gppnetwork.org>;tag=xdgZnFBF
To: < sip:[redacted]@ims.mnc.mcc.3gppnetwork.org>;tag=dfp5hc2d
CSeq: 1 SUBSCRIBE
[Truncated]Contact: < sip:username_nc_1c8_64e72b96_1686af34_k0t1HdtXaXh314caIpg2r0J7M75pQFh+mYw3Dy6UBP2dK0eYeNmfX6u4JEJ3CrWlUxj+w00qHqUs8t010g3aP1BrkG5NBaBHYHTwPo
Expires: 60000
P-Asserted-Identity: < sip:[redacted]-scscf01.ims.mnc.mcc.3gppnetwork.org>
Content-Length: 0

```

Figure 22. Disclosure of DNS names

SIP OPTIONS is another message that may disclose additional information to malefactors. Please refer to Figure 23 where such message discloses S-CSCF DNS name in From and P-Asserted-Identity headers, while User-Agent header allows malefactor to fingerprint vendor of hardware used in the network.

No.	Time	Source	Destination	Protocol	Length	CSeq	Info
7	48.475626980	[redacted]	[redacted]	SIP	842	1	OPTIONS Request: OPTIONS sip

```

Encapsulating Security Payload
User Datagram Protocol, Src Port: 9950, Dst Port: 7200
Session Initiation Protocol (OPTIONS)
Request-Line: OPTIONS sip:[redacted]:60:3550:E719]:7200;transport=udp SIP/2.0
Message Header
Via: SIP/2.0/UDP [redacted]:60:0000:0022]:9900;branch=z9hG4bKqj1rfm4lnmo9pa5yo9jr518;Role=3;Hpt=8ff2_36;X-HwD1m=4
Record-Route: < sip:[redacted]:60:0000:0022]:9900;lr;hpt=nm_222_643d3e84_b05b77c_ex_8ff2_16;Ctxid=4;TRC=ffffffff-ffffffff>
Call-ID: asbcik4lvs1kykk177j0j019j179eyo7q8S.5.114.ims.mnc.mcc.3gppnetwork.org
[Generated Call-ID: asbcik4lvs1kykk177j0j019j179eyo7q8S.5.114.ims.mnc.mcc.3gppnetwork.org]
From: < sip:scscf[redacted]-ims.mnc.mcc.3gppnetwork.org>;tag=7d98dded
To: < sip:[redacted]@ims.mnc.mcc.3gppnetwork.org>
CSeq: 1 OPTIONS
Max-Forwards: 69
User-Agent: HUAWEI_CSCF_PrePaging
P-Asserted-Identity: < sip:scscf[redacted]-ims.mnc.mcc.3gppnetwork.org>
Content-Length: 0

```

Figure 23. Hardware fingerprinting and disclosure of DNS names in SIP OPTIONS received from P-CSCF

In some cases, it is also possible to gather Cell-Id of other subscriber. Figure 24 shows how this info is disclosed in incoming SIP PRACK during call setup.

59	2021-12-27 10:51:05,967669	[redacted]	[redacted]	SIP/SDP	812	Status: 183 Session Prog
60	2021-12-27 10:51:06,011233	[redacted]	[redacted]	TCP	116	6060 + 6301 [ACK] Seq=908
61	2021-12-27 10:51:06,011252	[redacted]	[redacted]	TCP	116	6060 + 6301 [ACK] Seq=908
62	2021-12-27 10:51:06,343276	[redacted]	[redacted]	SIP	1004	Request: PRACK sip:[redacted]

```

> Frame 62: 1004 bytes captured (1004 bytes) on interface 0, time 10.5106343276 sec
> Linux capture filter: <>
> Internet Protocol Version 6, Src: [redacted], Dst: [redacted]
> Encapsulating Security Payload
> Transmission Control Protocol, Src Port: 6060, Dst Port: 6301, Seq: 9083, Ack: 5818, Len: 887
> Session Initiation Protocol (PRACK)
Request-Line: PRACK sip:[redacted]:6300 SIP/2.0
Message Header
Via: SIP/2.0/TCP [redacted]:6060;oc-algo="loss";oc;branch=z9hG4bKmavodi-0-264-1e1-1-2000000-b15100
Max-Forwards: 68
From: sip:[redacted]@ims.mnc.mcc.3gppnetwork.org;tag=mavodi-__rwuszztvvxx_0-10d-d4-5-ffffffff-149b
To: < tel:[redacted];phone-context=ims.mnc.mcc.3gppnetwork.org>;tag=6ea49803
Call-ID: FA163EF6B208-13ca-137c6700-d93110-61c97361-da2cc
[Generated Call-ID: FA163EF6B208-13ca-137c6700-d93110-61c97361-da2cc]
CSeq: 2 PRACK
RAck: 1 1 INVITE
Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
User-Agent: [redacted]
P-Access-Network-Info: 3GPP-E-UTRAN-FDD;local-time-zone="2021-12-27T10:51:06.343276+00:00";utran-cell-id-3gpp=[redacted]
access-type: 3GPP-E-UTRAN-FDD
local-time-zone="2021-12-27T10:51:06.343276+00:00"
utran-cell-id-3gpp: 3900170007140e
Content-Length: 0

```

Figure 24. Location disclosure

4.2.2. Incorrect anonymous call implementation

Most networks have a function for anonymous calls. Subscribers can prefix the called number with a command, e.g.*31# and their identity will be hidden from the receiving party.

In some of the networks where anonymous calls are supported, incoming SIP INVITE messages contained the identifier of the caller when establishing anonymous call, giving malefactor the ability to de-anonymize caller. At the same time, in some networks, these messages were sanitized from such details. This shows that there are ways to make calls truly anonymous, but MNOs often overlook this feature.

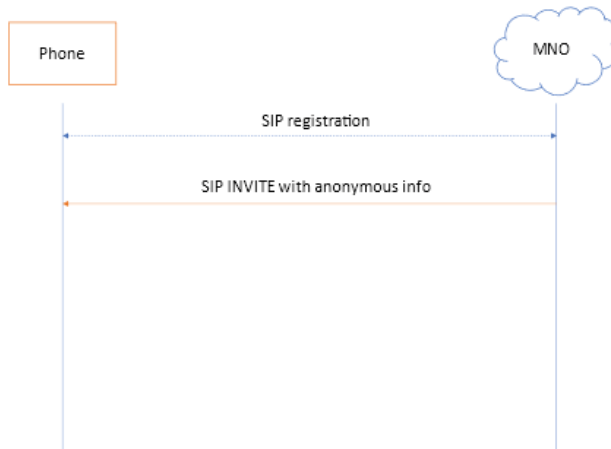


Figure 25. Subscriber info in anonymous call scheme

```

0_000763316 Request: INVITE sip: de6680
0_001060936 Status: 100 Trying
0_001062503 Destination unreachable (Port unreachable)
0_003578735 Status: 183 Session Progress
7_609516574 Request: PRACK sip: de6680

Encapsulating Security Payload
Transmission Control Protocol, Src Port: 9950, Dst Port: 44843, Seq: 2041, Ack: 1, Len: 599
[3 Reassembled TCP Segments (2639 bytes): #1(1020), #2(1020), #3(599)]
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip: de6680 SIP/2.0
Message-Header
Via: SIP/2.0/TCP :9900;branch=z9hG4bK3rb12d9bfrh3dh02c09b6bf;Role=3;Hpt=8f52_36
Record-Route: <sip: :9900;transport=tcp;lr;Hpt=nw_156_650412a7_17d2b543_ex_8f52_16;CxtId=4;TRC=ffffffff-ffffffff;X-HwB2bUaCookie=13813>
Call-ID: asbcpgdm701oj5m1cg2o72270526jo2v6g0o0
[Generated Call-ID: asbcpgdm701oj5m1cg2o72270526jo2v6g0o0-173_77_331]
From: <tel: 2390;noa=national;srvattri=national;phone-context= >;tag=o510qs50
SIP From address: tel: 2390;noa=national;srvattri=national;phone-context=
SIP from tag: o510qs50
To: :1906;phone-context=ims.mnc .3gppnetwork.org>
CSeq: 1 INVITE
Accept: application/sdp,application/3gpp-ims+xml,application/vnd.3gpp.state-and-event-info+xml
Allow: INVITE,ACK,OPTIONS,CANCEL,BYE,UPDATE,INFO,REFER,NOTIFY,MESSAGE,PRACK
Contact: <sip: :9900;Dsp=ee6a-200;Hpt=nw_156_650412a7_17d2b543_ex_8f52_16;CxtId=4;TRC=ffffffff-ffffffff>;+g.3gpp.icsi-ref="urn%3Aurn-7%3A
Contact URI: sip: :9900;Dsp=ee6a-200;Hpt=nw_156_650412a7_17d2b543_ex_8f52_16;CxtId=4;TRC=ffffffff-ffffffff
Contact parameter: +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
Contact parameter: +g.3gpp.mid-call
Max-Forwards: 62
Supported: timer,tdialog,100rel,gruu
User-Agent: Samsung IMS 6.0 (SM-N950F Android 9)
Session-Expires: 1800
Min-SE: 600
Privacy: id
P-Called-Party-ID: <sip: :1906@ims.mnc .mcc .3gppnetwork.org>
P-Early-Media: supported,gated
P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
P-Asserted-Service-Info: access-domain=ims-lte
Feature-Caps: *+g.3gpp.srvcc;+g.3gpp.mid-call;+g.3gpp.srvcc-alerting
Recv-Info: g.3gpp.state-and-event-info
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel",*;explicit;require;+g.3gpp.accesstype="cellular2",*;explicit;require;
Content-Length: 977
Content-Type: application/sdp
  
```

Figure 26. Subscriber info in anonymous call

There are some specific things that you can introduce in the MNO to deal with network info disclosure like node fingerprinting and subscriber info, but it all boils down to filtering network or VoLTE-specific identifiers from SIP packets on the network-to-subscribers border.

4.2.3. Lack of SIP Flood protections

Another example of disregard: Protection from SIP protocol flooding on the IMS core nodes. It is very common to combat SIP flood by implementing a rate limit for the SIP REGISTER or SIP INVITE, as IP-Exchanges open to internet traffic can easily be targeted for DDoS. Unfortunately, protections against such attacks are not commonly found in the IMS environments that we have tested so far. On IMS bearer, such floods can be used not only for network DoS, but also for targeted DoS attacks on subscribers, see Figure 27 and Figure 28. **This variation of attack was reported in [7] in 2020.**



Figure 27. SIP flood scheme

No.	Time	Source	Destination	Info
8	74.343498613			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
11	74.917164917			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
15	75.463586609			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
21	76.184695888			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
27	76.879419465			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
32	77.459209547			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
38	78.060728583			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
44	78.615428218			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
49	79.087446079			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
53	79.591421564			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
58	80.005309017			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
63	80.499333226			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
67	80.983380692			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
72	81.523371150			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
77	82.076020913			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
84	82.651234762			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
88	83.167275787			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
94	83.605018447			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
98	84.139364667			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
103	84.591678281			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
109	85.059333307			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
113	85.563345018			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
119	86.019245298			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
124	86.499343895			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
130	86.983280880			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
135	87.423232560			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
142	87.875410066			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
146	88.315465886			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
152	88.731553170			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
155	89.239233828			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
163	89.772295459			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
166	90.295346812			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
176	90.919461505			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org
179	91.415688593			Request: INVITE tel:06;phone-context=ims.mnc.mcc.3gppnetwork.org

Figure 28. SIP flood

One of the options for the malefactor is to send a lot of SIP invites for one particular subscriber. As a result, no incoming calls can get through to the target. It also should be noted, that sending a lot of INVITE messages without any continuation may result in a so-called “silent call” attack. While the phone’s modem constantly receives and processes these messages, no calls are displayed. As a result, it is possible for malefactor to stealthily drain the phone’s battery. **This specific vulnerability was originally reported in [6] in 2015.**

Time	Source	Destination	Protocol	Length	Info
0.088959639			SIP/SDP	858	Request: INVITE tel:
0.362133131			SIP	390	Status: 100 Trying
0.748406101			SIP/SDP	858	Request: INVITE tel:
0.845753248			SIP	390	Status: 100 Trying
0.845753591			SIP	494	Status: 481 Call/Tra
1.355600249			SIP	494	Status: 481 Call/Tra
1.424728043			SIP/SDP	858	Request: INVITE tel:
1.499565705			SIP	390	Status: 100 Trying
1.499566282			SIP	494	Status: 481 Call/Tra
1.989812185			SIP	494	Status: 481 Call/Tra
2.060622009			SIP/SDP	858	Request: INVITE tel:
2.346017381			SIP	494	Status: 481 Call/Tra
2.584725600			SIP/SDP	858	Request: INVITE tel:
2.646020102			SIP	390	Status: 100 Trying
2.646020496			SIP	494	Status: 481 Call/Tra
2.916095232			SIP/SDP	1478	Status: 183 Session
2.997392314			SIP	494	Status: 481 Call/Tra
3.129719134			SIP	494	Status: 481 Call/Tra
3.288644916			SIP/SDP	858	Request: INVITE tel:
3.349730518			SIP	390	Status: 100 Trying
3.349731551			SIP	494	Status: 481 Call/Tra
3.425997498			SIP/SDP	1478	Status: 183 Session
3.853380267			SIP	494	Status: 481 Call/Tra
3.884863244			SIP/SDP	858	Request: INVITE tel:
4.135993795			SIP	494	Status: 481 Call/Tra
4.349844023			SIP	494	Status: 481 Call/Tra
4.404310572			SIP/SDP	858	Request: INVITE tel:
4.409737424			SIP/SDP	1478	Status: 183 Session
4.470243575			SIP	390	Status: 100 Trying
4.470244823			SIP	494	Status: 481 Call/Tra
4.875590469			SIP	494	Status: 481 Call/Tra
4.966020542			SIP	494	Status: 481 Call/Tra
4.989696060			SIP	494	Status: 481 Call/Tra
5.157483537			SIP/SDP	858	Request: INVITE tel:
5.884462832			SIP/SDP	858	Request: INVITE tel:
5.955618223			SIP	390	Status: 100 Trying
5.955618603			SIP	494	Status: 481 Call/Tra

```

> Frame 4: 858 bytes on wire (6864 bits), 858 bytes captured (6864 bits) on interface enx0
> Ethernet II, Src: 0c:5b:8f:27:9a:64 (0c:5b:8f:27:9a:64), Dst: HuaweiTe_e3:9d:c3 (c8:c2:fd
> Internet Protocol Version 4, Src: [REDACTED]
> Encapsulating Security Payload
> User Datagram Protocol, Src Port: 6200, Dst Port: 9900
> Session Initiation Protocol (INVITE)
  > Request-Line: INVITE tel:[REDACTED]906;phone-context=ims.mnc[REDACTED].mcc[REDACTED].3gppnetwork.org
  > Message Header
    > Via: SIP/2.0/UDP [REDACTED]:7200;branch=z9hG4bK-nGjIGQLrs578sGoWI2Zr8CN3MnbhUbm2
    > Max-Forwards: 70
    > Route: <sip:[REDACTED]:9900;lr>
    > Contact: <sip:[REDACTED]8033@[REDACTED]:7200>;+g.3gpp.icsi-ref="urn:3Aurn-7X3A3gpp
    > To: tel:[REDACTED]906;phone-context=ims.mnc[REDACTED].mcc[REDACTED].3gppnetwork.org
    > From: <sip:[REDACTED]2390@ims.mnc[REDACTED].mcc[REDACTED].3gppnetwork.org>;tag=EJpPx56
    > Call-ID: [REDACTED]
  
```

Figure 29. Subscriber DoS via SIP flood, attacker's side

```

79.664455520 SIP/SDP 754 Request: INVITE
79.664765074 SIP 546 Status: 100 Try
79.664767696 ICMP 574 Destination unr
79.665428375 SIP/SDP 466 Status: 183 Ses
79.682983875 SIP/SDP 466 Status: 183 Ses
79.697508828 SIP/SDP 466 Status: 183 Ses
99.786162409 SIP/SDP 466 Status: 183 Ses
99.800678140 SIP/SDP 466 Status: 183 Ses
99.805150812 SIP 690 Request: CANCEL
99.805733502 SIP 562 Status: 200 OK
99.805739591 ICMP 590 Destination unr
99.806069263 SIP 658 Status: 487 Req
99.811029812 SIP 562 Request: ACK si
99.811047561 ICMP 590 Destination unr
117.1353672... SIP/SDP 754 Request: INVITE
117.1357026... SIP 546 Status: 100 Try
117.1357086... ICMP 574 Destination unr
117.1369755... SIP/SDP 466 Status: 183 Ses
117.1417849... SIP/SDP 466 Status: 183 Ses
117.1517196... SIP/SDP 466 Status: 183 Ses
117.1580413... SIP/SDP 466 Status: 183 Ses
134.0861494... SIP/SDP 466 Status: 183 Ses
134.0875167... SIP 690 Request: CANCEL
134.0931876... SIP 562 Status: 200 OK
134.0932021... ICMP 590 Destination unr
134.0935420... SIP 658 Status: 487 Req
134.0938509... SIP 562 Request: ACK si
134.0938568... ICMP 590 Destination unr
134.1063326... SIP/SDP 746 Request: INVITE
159.2689787... SIP 546 Status: 100 Try
159.2695383... SIP/SDP 466 Status: 183 Ses
159.2706553... ICMP 574 Destination unr
159.2745509... SIP/SDP 466 Status: 183 Ses

```

```

User Datagram Protocol, Src Port: 36502, Dst Port: 47290
Internet Protocol Version 4, [redacted]
Encapsulating Security Payload
Transmission Control Protocol, Src Port: 9952, Dst Port: 42567, Seq: 2041, Ack:
[3 Reassembled TCP Segments (2683 bytes): #7501(1020), #7505(1020), #8983(643)]
Session Initiation Protocol (INVITE)
Request-Line: INVITE sip:[redacted]:42
Message Header
Via: SIP/2.0/TCP [redacted]:9900;branch=z9hG4bKextpxcozdetdsaxxptfo9ce:
Record-Route: <sip:[redacted]:9900;transport=tcp;lr;hpt=nw_526_6508515:
Call-ID: asbctuc16tbsb6wbuiksx62rb6b1k6tcxk@[redacted]
[Generated Call-ID: asbctuc16tbsb6wbuiksx62rb6b1k6tcxk@[redacted]]
From: <tel:[redacted]2390;oa=national;srvattri=national;phone-context=[redacted]>

```

Figure 30: Subscriber DoS via SIP flood, victim's side

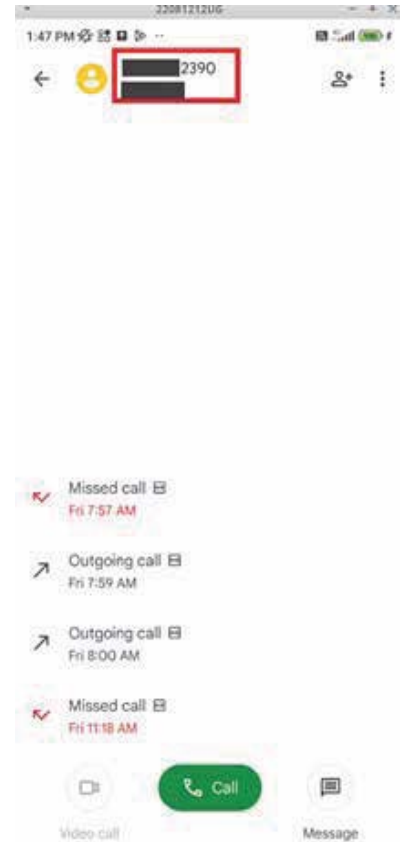


Figure 31: Subscriber DoS via SIP flood, phone with just a handful of missed calls during all this time.

Time	Source	Destination	P-Asserted-Identity	Info
211.6438213...			<sip:[redacted]1448@ims.mnc011	Request: INVITE sip:d6e1fd0a-
289.7494971			<sip:[redacted]2390@ims.mnc010	Request: INVITE sip:d6e1fd0a-
317.2177270...			<sip:[redacted]2390@ims.mnc010	Request: INVITE sip:d6e1fd0a-
343.4035243...			<sip:[redacted]2390@ims.mnc010	Request: INVITE sip:d6e1fd0a-
381.9505183...			<sip:[redacted]2390@ims.mnc010	Request: INVITE sip:d6e1fd0a-
419.2444249...			<sip:[redacted]2390@ims.mnc010	Request: INVITE sip:d6e1fd0a-
458.7084409...			<sip:[redacted]1448@ims.mnc011	Request: INVITE sip:d6e1fd0a-

Figure 32: INVITEs from other phones are not routed while messages are being sent by malefactor

4.2.4. No sanitation of experimental headers

SIP messages are text-based and may include a lot of different fields depending on specific SIP usage. Some of these are only used in IP-telephony, some pertain to VoLTE/VoWiFi and some are formally deprecated. A prime example of this is the experimental (spelled X-something) fields. In many cases, such fields were not

filtered by SIP proxies employed in the MNOs that we tested, resulting in a situation where unneeded deprecated header from SIP INVITE sent towards the network was copied verbatim into the SIP INVITE sent from network to the target subscriber.

This allows malefactors to implement stealth tunnelling attacks in IMS infrastructure by sending SIP INVITEs with additional data. The receiving side may drop the call and respond with a new SIP INVITE to the original sender. As SIP call is never established during this exchange, and signaling traffic on IMS bearer is not billed, this allows for unbilled messaging through the operator's core network nodes. Such an attack is convenient for malefactor as all the routing is done by the MNO. **This vulnerability was originally reported in [5] in 2015.**

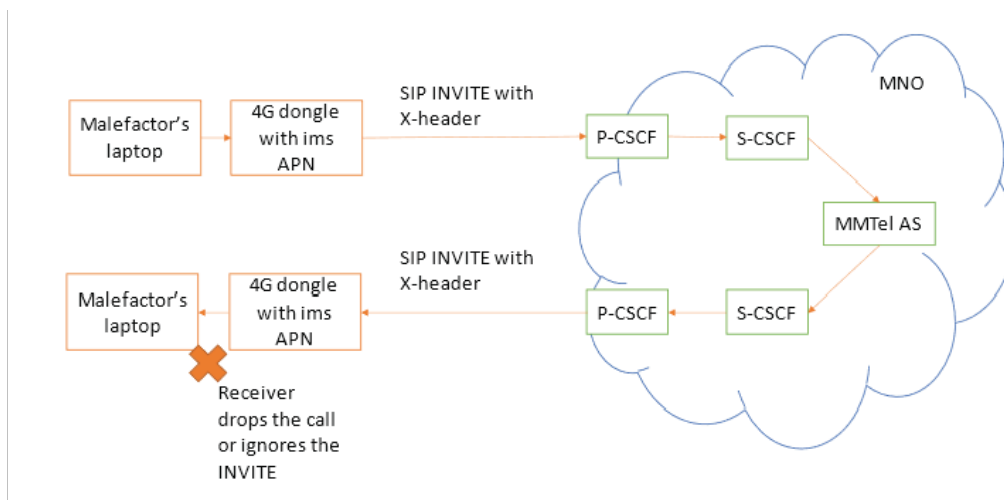


Figure 33: Sending unbilled data in INVITE scheme (1)

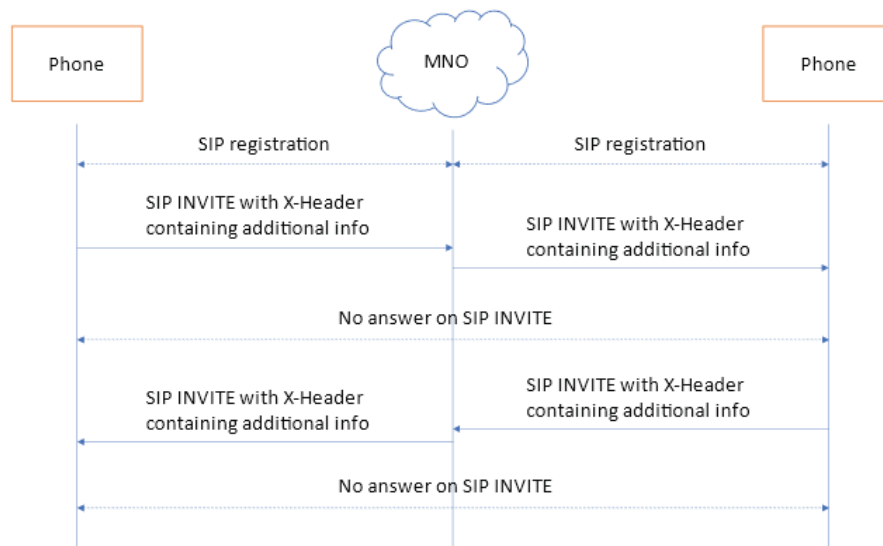


Figure 34: Sending unbilled data in INVITE scheme (2)

```

Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:[redacted]:44843 SIP/2.0
  Message Header
    Via: SIP/2.0/TCP [redacted]:9900;branch=z9hG4bK4sJ434rm91m199mpmk9]tsnp;Role=3;Hpt=9002_36
    Record-Route: < sip:[redacted]:9900;transport=tcp;lr;Hpt=nw_235_650440ad_17d700b0_ex_9002_16;CxtId=4;TRC=ffffff-ffffff>
    Call-ID: asbcyhgfha66h11ldgf4fih1q1agdhly71e [redacted]
    [Generated Call-ID: asbcyhgfha66h11ldgf4fih1q1agdhly71e [redacted]]
    From: <tel:[redacted]:2390;noa=national;srvattri=national;phone-context=[redacted];tag=qal0fawg>
    SIP from address: tel:[redacted]:2390;noa=national;srvattri=national;phone-context=[redacted]
    SIP from tag: qal0fawg
    To: <tel:[redacted]:906>;phone-context=ims.mcc [redacted].mcc [redacted].3gppnetwork.org
    SIP to address: tel:[redacted]:906
    CSeq: 1 INVITE
    Accept: application/sdp,application/3gpp-ims+xml,application/vnd.3gpp.state-and-event-info+xml
    Allow: INVITE,ACK,CANCEL,BYE,UPDATE,PRACK,MESSAGE,REFER,NOTIFY,INFO,OPTIONS
    Contact: < sip:[redacted]:9900;Dsp=eb9a-200;Hpt=nw_235_650440ad_17d700b0_ex_9002_16;CxtId=4;TRC=ffffff-ffffff>;q=1
    Contact URI: sip:[redacted]:9900;Dsp=eb9a-200;Hpt=nw_235_650440ad_17d700b0_ex_9002_16;CxtId=4;TRC=ffffff-ffffff
    Contact parameter: q=1
    Contact parameter: +g.3gpp.icsi-ref="urn:urn-7:3gpp-service.ims.icsi.mmtel"
    Contact parameter: +g.3gpp.mid-call
    Max-Forwards: 62
    Supported: timer,tdialog,100rel,replaces,from-change,histinfo,tdialog
    User-Agent: SM-A217F-UA2 Samsung IMS 6.0
    Session-Expires: 1800
    Min-SE: 600
    P-Asserted-Identity: < sip:[redacted]:2390@ims.mcc [redacted].mcc [redacted].3gppnetwork.org>,<tel:[redacted]:2390>
    SIP PAI Address: sip:[redacted]:2390@ims.mcc [redacted].mcc [redacted].3gppnetwork.org
    P-Called-Party-ID: < sip:[redacted]:906@ims.mcc [redacted].mcc [redacted].3gppnetwork.org>
    P-Early-Media: supported,gated
    P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
    X-Header: Charging Abuse Checks via SIP tunneling mechanisms: INVITE X-Header
    P-Asserted-Service-Info: access-domain=ims-ite
    Feature-Caps: *;+g.3gpp.srvcc;+g.3gpp.mid-call;+g.3gpp.srvcc-alerting
    Recv-Info: g.3gpp.state-and-event-info
    Accept-Contact: *;+g.3gpp.icsi-ref="urn:urn-7:3gpp-service.ims.icsi.mmtel",*;explicit;require;+g.3gpp.accesstype="cel"
    Content-Length: 306
    Content-Type: application/sdp
  Message Body
    Session Description Protocol
  
```

Figure 35. Sending unbilled data in INVITE

4.2.5. Impersonated SMS

In the 4G and 5G context, the SIP protocol is also used for SMS messaging.

As such, malefactors can send mobile-originated SMS messages to the Short Message Service Center. We found that it may be possible to spoof the origin identity to send bulk SMS while bypassing any billing.

This impersonated messaging can be taken a step further, as in certain operators it was possible to successfully send mobile terminated SMS posing as SMS Center.

Source	Destination	Protocol	Info
[redacted]	[redacted]	GSM SMS Request	MESSAGE sip:[redacted]:906@ims.m
[redacted]	[redacted]	SIP	Status: 200 OK

```

Frame 3: 1002 bytes on wire (8016 bits), 1002 bytes captured (8016 bits) on interface II, Src: 0c:5b:8f:27:9a:64 (0c:5b:8f:27:9a:64), Dst: HuaweiTe_e3:9d:c3
Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
Encapsulating Security Payload
User Datagram Protocol, Src Port: 6200, Dst Port: 9900
Session Initiation Protocol (MESSAGE)
  Request-Line: MESSAGE sip:[redacted]:906@ims.mcc [redacted].3gppnetwork.org;user=phone
  Message Header
    [Expert Info (Warning/Undecoded): Trailing stray characters]
    Via: SIP/2.0/UDP [redacted]:5060;branch=z9hG4bK-KeoXhQfQgzHCYaNcwmfCLU2gJK
    Max-Forwards: 70
    Contact: < sip:[redacted]:2390@ims.mcc [redacted].mcc [redacted].3gppnetwork.org>;+g.3gpp.mid-call;+g.3gpp.icsi-ref="urn:urn-7:3gpp-service.ims.icsi.mmtel"
    To: < sip:[redacted]:906@ims.mcc [redacted].mcc [redacted].3gppnetwork.org;user=phone>
    From: < sip:[redacted]:2390@ims.mcc [redacted].mcc [redacted].3gppnetwork.org>;tag=ca4PHAfZ
    Call-ID: ca4PHAfZ
    [Generated Call-ID: ca4PHAfZ]
    CSeq: 1 MESSAGE
    Allow: MESSAGE
    Supported: path,gruu
    Request-Disposition: no-fork
    Accept-Contact: *;+g.3gpp.smsip
    User-Agent: SM-A217F-UA2 Samsung IMS 6.0
    P-Preferred-Identity: < sip:[redacted]:2390@ims.mcc [redacted].mcc [redacted].3gppnetwork.org>
    P-Access-Network-Info: 3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=[redacted]
    Content-Type: application/vnd.3gpp.sms
    Content-Length: 36
  Message Body
    GSM A-I/F RP - RP-DATA (Network to MS)
    GSM SMS TPDU (GSM 03.40) SMS-DELIVER
    0... .. = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/
    .0... .. = TP-UDHI: The TP UD field contains only the short message
    .0... .. = TP-SRI: A status report shall not be returned to the SME
    ... 0... = TP-LP: The message has not been forwarded and is not a spawn
    ... .1... = TP-MMS: No more messages are waiting for the MS in this SC
    ... ..00 = TP-MTI: SMS-DELIVER (0)
    IP-Originating-Address - ([redacted]:3418)
    TP-PIU: 0
    TP-DCS: 0
    TP-Service-Centre-Time-Stamp
    TP-User-Data-Length: (4) depends on Data-Coding-Scheme
    TP-User-Data
    SMS text: Test
  Session Initiation Protocol (SIP as raw text)
  
```

Figure 36. Spoofing source in MT SMS attacker's side

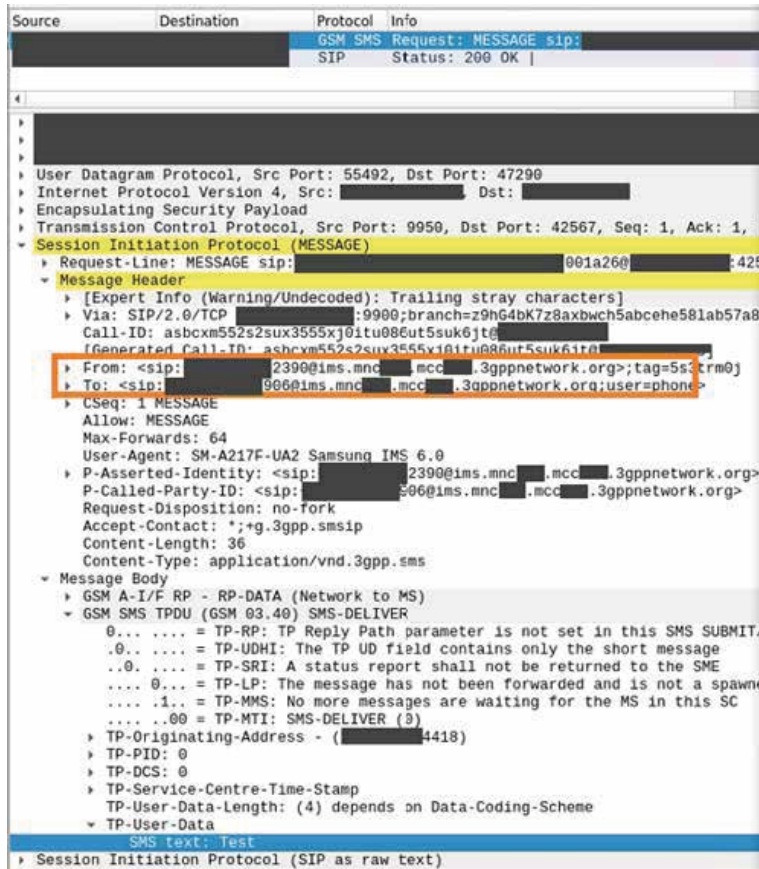


Figure 37: Spoofing source in MT SMS victim's side

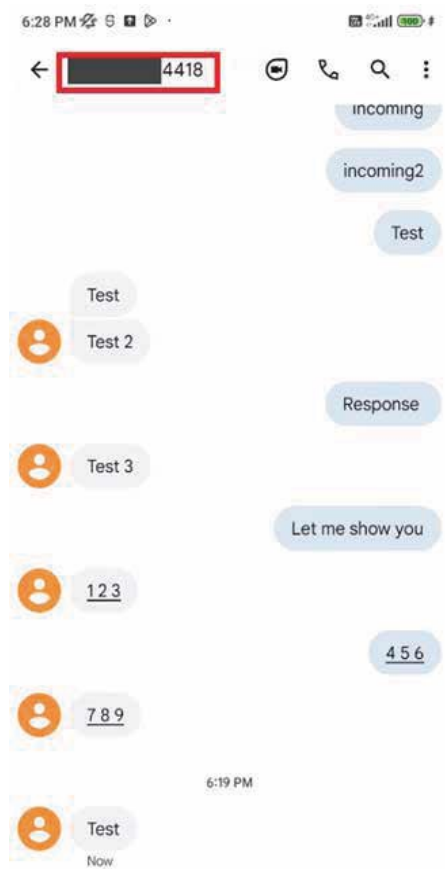


Figure 38: Spoofing source in MT SMS phone

Again, it feels like some operators are not prepared to put SMS via SIP through the same scrutiny as usual SMS.

05. Recommendations for enhancing VoLTE security:

The security of SIP and all adjacent technologies is considered quite mature. GSMA documents [1], [2] describe possible threats and ways to deal with them. Despite this, we see that a lot of MNOs seem to disregard it for one specific attack vector – traffic coming from subscriber's phones. To fix this blind spot we recommend going through following steps:

- First, there is a need to assess the current situation. To do so MNOs would need to perform security audit of VoLTE/VoWiFi connections to IMS. This will show which of the vulnerabilities mentioned above are applicable and outline the general protection level of the network.

- Next step is to enable protection and implement monitoring on these interfaces. While blocking of malicious messages is self-explanatory, having a comprehensive monitoring solution on top of it is crucial for visibility, rapid detection, and mitigation of threats.

GSMA recommends deploying Access Session Border Controller (A-SBC) fronted by an IP firewall to protect the network. It is also recommended to have cross-protocol correlations between SIP signalling and SS7, Diameter and HTTP/2 to find possible malefactors.

Still, many vulnerabilities stem from incorrect configurations, such as direct connections between phones enabled by improper network segmentation. We also believe that even if a dedicated A-SBC is not employed, most protection measures can still be implemented using configurable SIP proxies, IP firewalls, and anti-fraud systems that handle SMS and calls. Thus, many of these issues can likely be addressed by activating existing features in already deployed hardware or through simple reconfiguration of current security measures.

Setting up a clear monitoring solution in this case, however, may be quite tricky, as it requires correlating data from several different nodes across the network.

Finally, it is important to continuously perform periodical reassessments, to help protect network post reconfigurations and or against newly discovered threats.

06. Future-proofing VoLTE / VoNR security

As the telecom industry pivots towards 5G, ensuring the security of VoLTE becomes even more critical. The next generation of networks promises enhanced capabilities but also brings new security challenges. Operators must adopt a proactive approach to security, implementing robust encryption, secure network architecture, and continuous monitoring to protect against emerging threats. The transition to 5G offers a unique opportunity to address the legacy security issues of VoLTE, ensuring a secure and resilient foundation for the future of telecommunications.

07. Terms and abbreviations

3GPP	- 3rd Generation Partnership Project
APN	- Access Point Name
A-SBC	- Access Session Border Controller
BGCF	- Breakout Gateway Control Function
BTS	- Base Transceiver Station
CS	- Circuit Switching
CS-MGW	- CS Media Gateway
(D)DoS	- (Distributed) Denial of Service
DNS	- Domain Name Service
FQDN	- Fully Qualified Domain Name
FTP	- File Transfer Protocol
GGSN	- Gateway GPRS Support Node
GSM	- GSM Association
HSS	- Home Subscriber Server
I-CSCF	- Interrogating Call Session Control Function
IMS	- IP Multimedia Subsystem
IP	- Internet Protocol
LTE	- Long-Term Evolution
MGCF	- Media Gateway Controller Function
MGW	- Media Gateway
MME	- Mobility Management Entity
MMTel AS	- Multimedia Telephony service Application Server
MNO	- Mobile Network Operator
MO-SMS	- Mobile Originating SMS
MSC	- Mobile Switching Center
MT-SMS	- Mobile Terminating SMS
P-CSCF	- Proxy Call Session Control Function
PGW	- Packet Gateway
PSTN	- Public Switched Telephone Network
PDN-GW	- Packet Data Network Gateway
RTP	- Real-time Transport Protocol
S-CSCF	- Serving Call Session Control Function
SGSN	- Serving GPRS Support Node
SGW	- Serving Gateway
SIP	- Session Initiation Protocol
SMS	- Short Message Service
SMS-C	- SMS Center

SS7	- Signalling System No. 7
SSH	- Secure Shell Protocol
USB	- Universal Serial Bus
VoIP	- Voice over Internet Protocol
VoLTE	- Voice over LTE
VoNR	- Voice over New Radio
VoWiFi	- Voice over WiFi

08. References

1. GSMA FS.38 SIP Network Security
2. GSMA FS.22 VoLTE Security Analysis and Recommendations
3. Novikov P. How to hijack a VoLTE network (Ekoparty, Buenos Aires, Argentina, 2023)
4. Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan Yuanjie Li, Songwu Lu, Xinbing Wang. Insecurity of Voice Solution VoLTE in LTE Mobile Networks. CCS'15, October 2015.
5. H.Kim, D. Kim, M. Kwon, H. Han, Y.J.D.Han, T. Kim, Y.Kim. Breaking and Fixing VoLTE, Exploiting Hidden Data Channels and Mis-implementations. CCS'15, October 2015.
6. Guan-Hua Tu, Chunyi Peng, Hongyi Wang, Chi-Yu Li, Songwu Lu. How Voice Call Technology Poses Security Threats in 4G LTE Networks. CCS'15, October 2015
7. Yu-Han Lu, Chi-Yu Li, Yao-Yu Li, Sandy Hsin-Yu Hsiao, Tian Xie, Guan-Hua Tu, Wei-Xun Chen. Ghost calls from operational 4G call systems: IMS vulnerability, call DoS attack, and countermeasure, 2020.

About SecurityGen

SecurityGen is a global company focused on cybersecurity for telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure safe and robust network operations. Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats.

Connect With Us

Email: contact@secgen.com

Website: www.secgen.com

UK | Italy | Czech Republic | Brazil | Mexico
India | South Korea | Malaysia | Egypt | Lebanon

*Published in: July 2024