SecurityGen

Telecom Security. Transcending Generations.

VoLTE

A history of disregard

Table of contents

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 specific subsystem used for voice calls, which is a part of control plane segment (CS-MGW) connected to the Public Switched Telephone Network (PSTN)

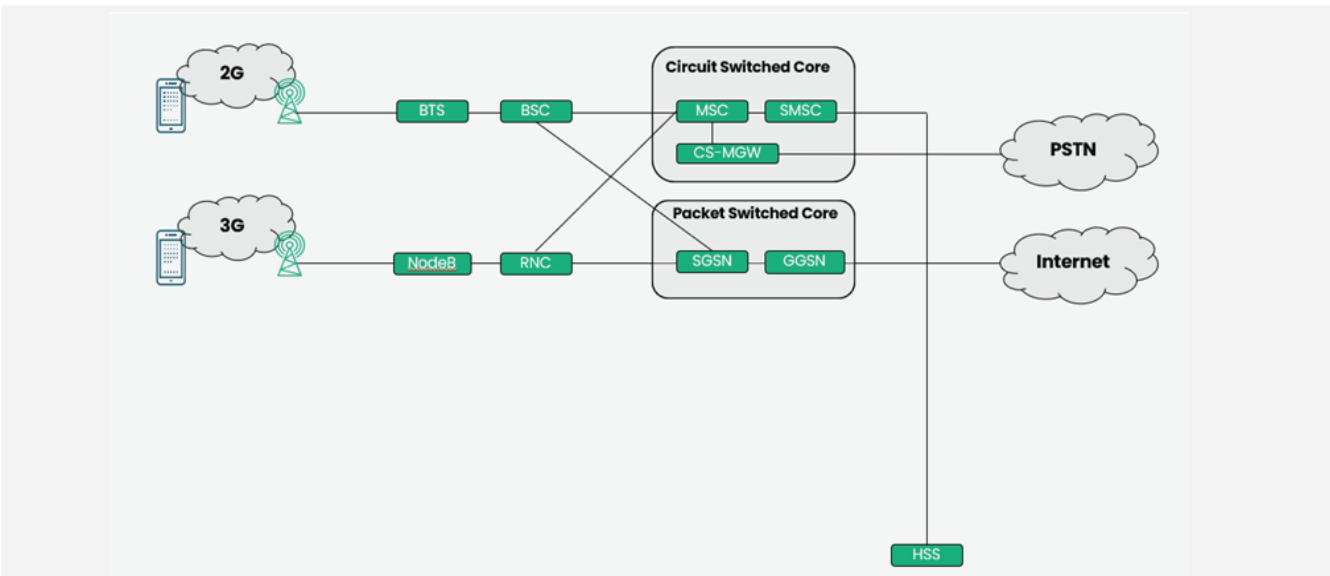


Figure 1. 2G and 3G telephony

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

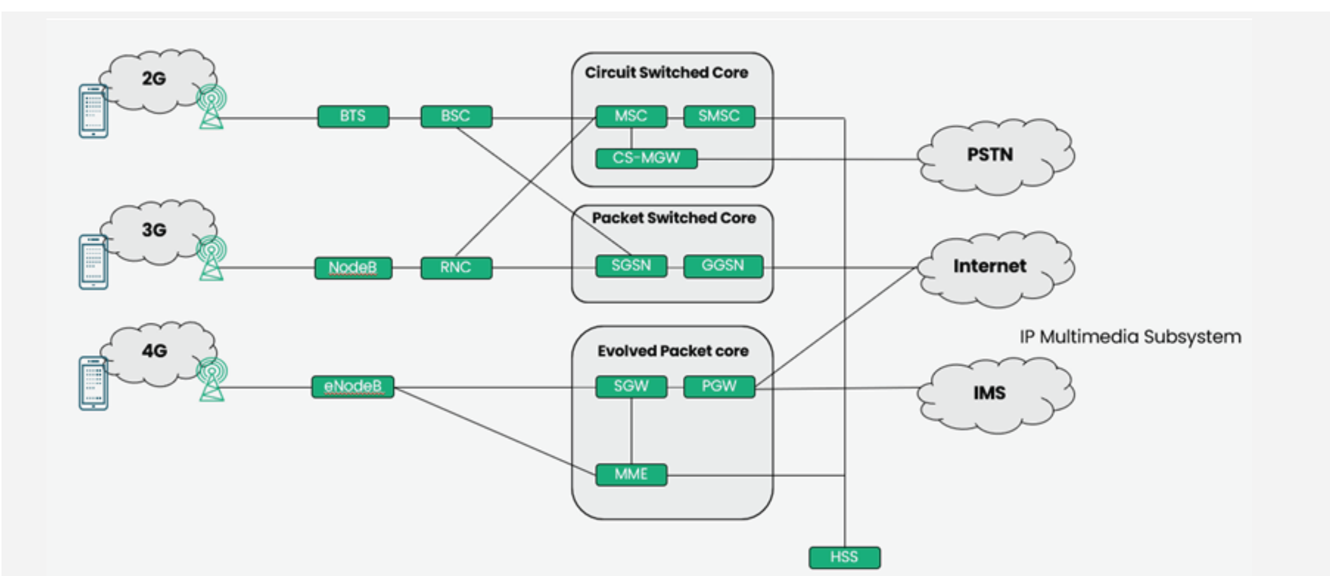


Figure 2. Place of IMS in mobile network

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.**

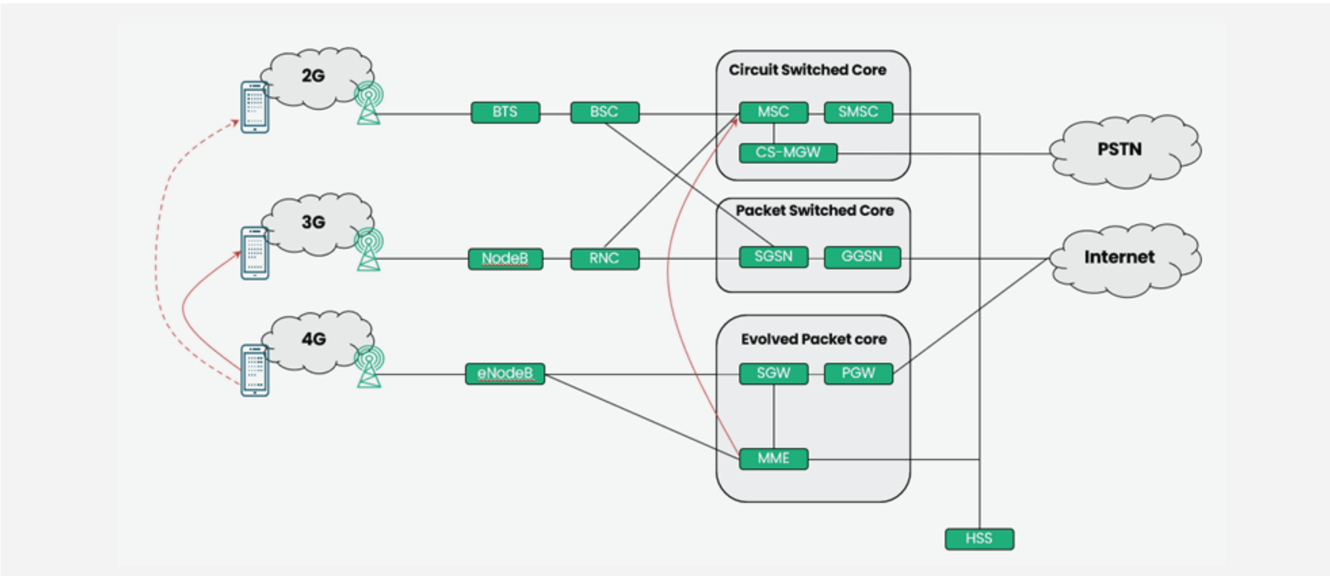


Figure 3. Voice call via CS-fallback

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".

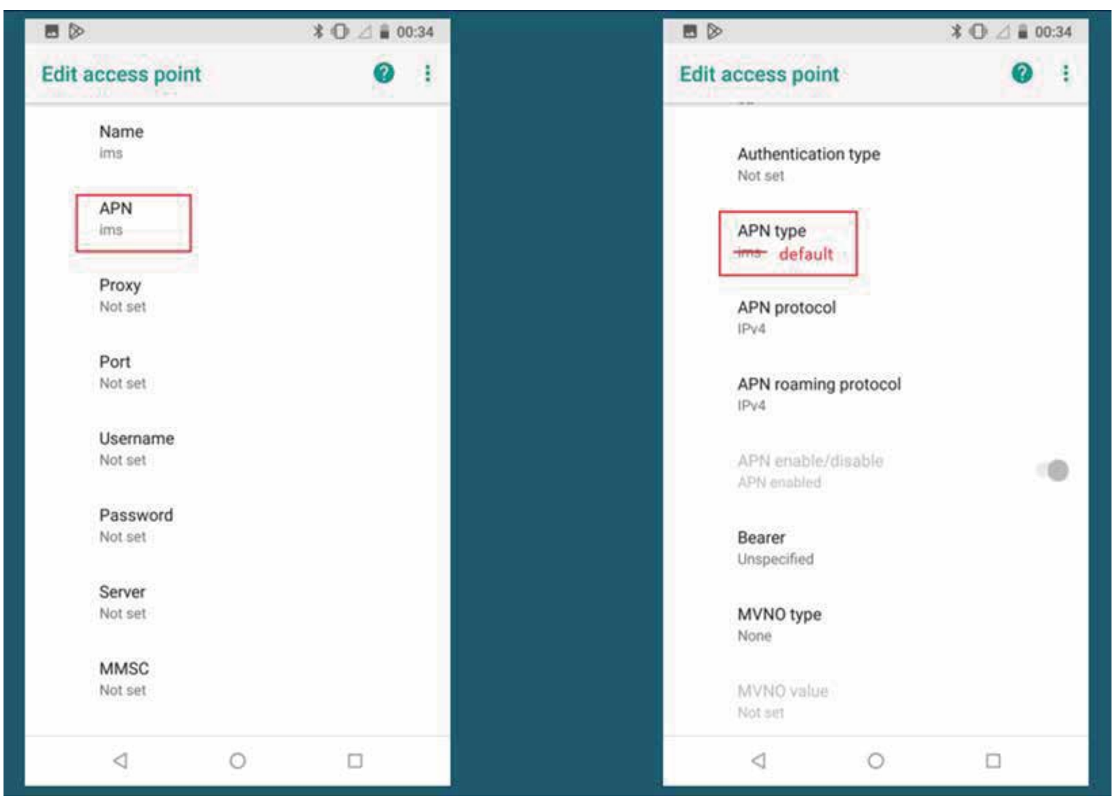


Figure 4. Using IMS APN for usual data connection to access IMS core

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.

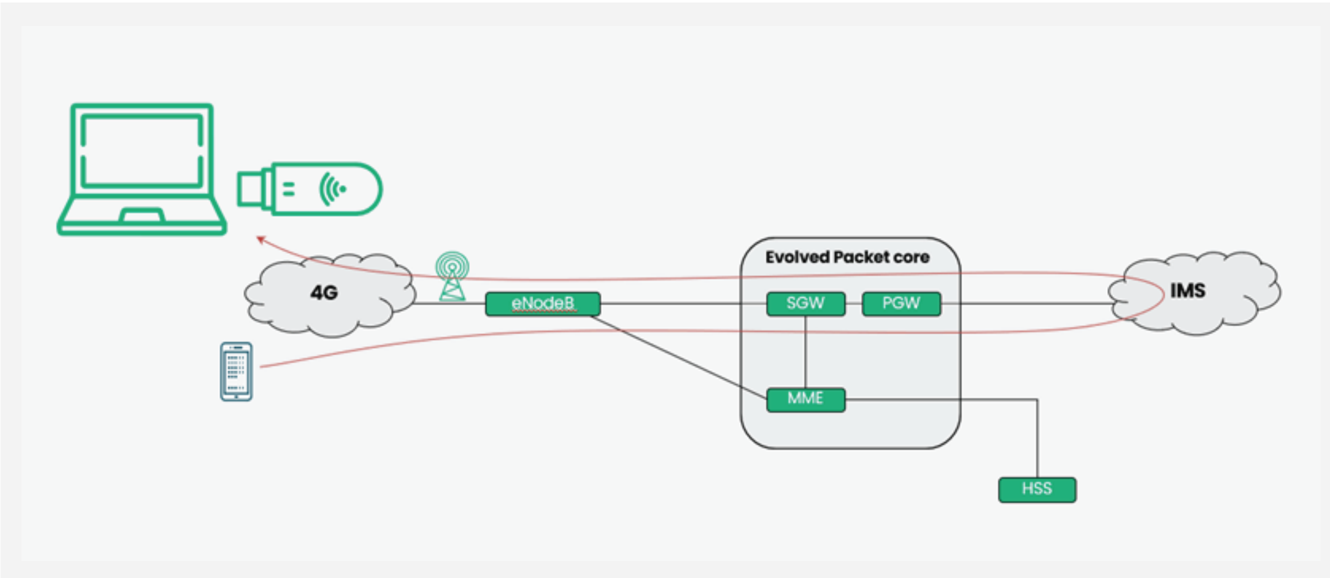


Figure 5. Using laptop for IMS connectivity

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

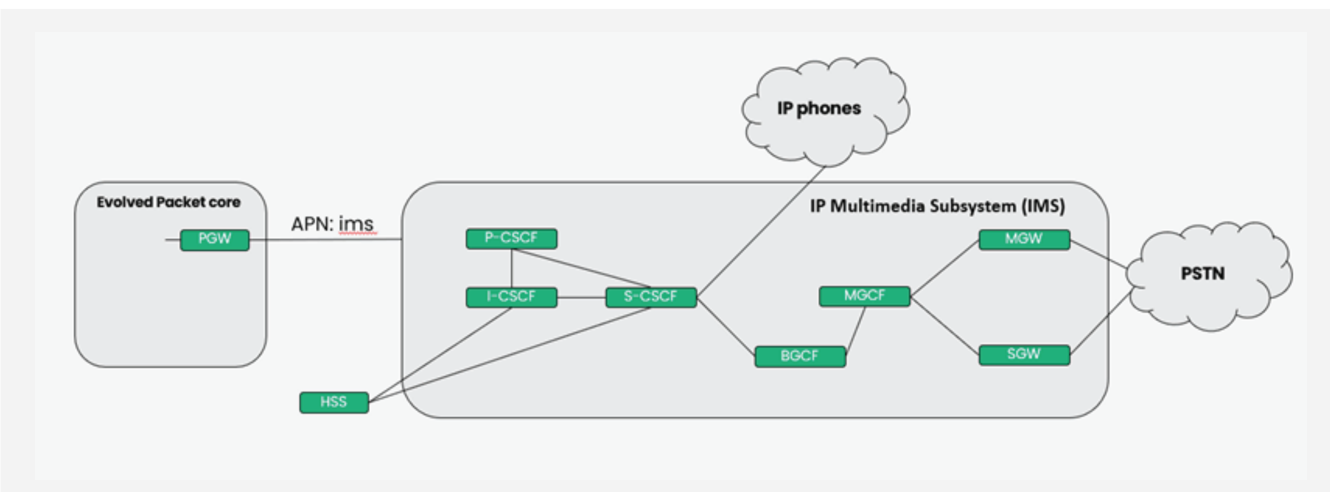


Figure 6. IMS structure

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

4.1 IP Connectivity

Once 'ims' APN is added, the subscriber's device will try to establish IP connectivity in form of an EPS bearer. Once it is set up, a separate network interface with access to the subnet with P-CSCF node is available to the device. Only P-CSCFs should be accessible using this interface.
This provokes some questions: Is it possible to address any other IPs in this subnet? Since it is a typical IP network, traditional scanning methods can be used, such as passive sniffing of received messages or active nmap scans.

4.1.1. Nmap scan

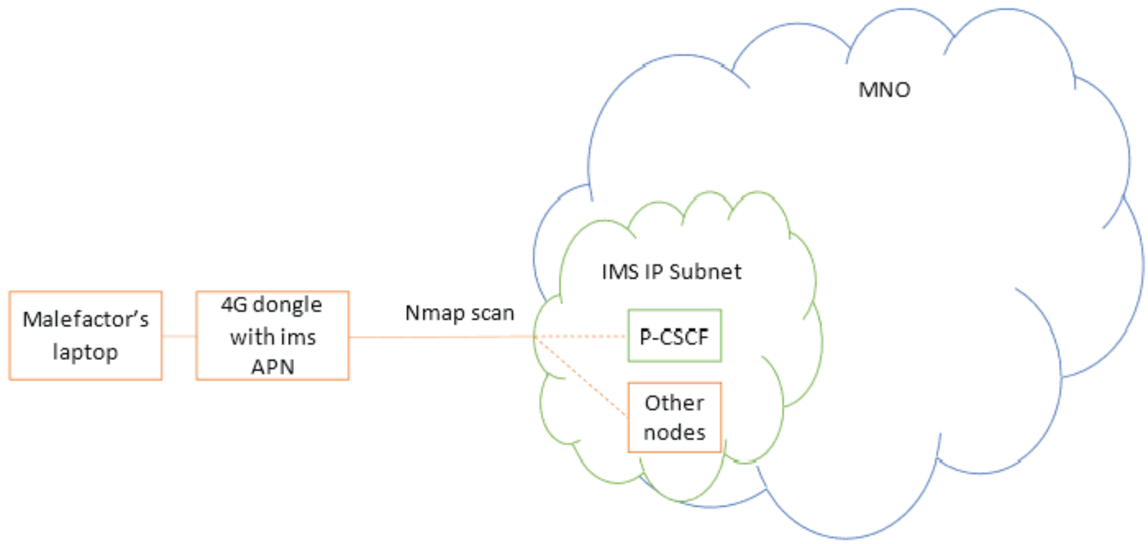


Figure 7: nmap scan scheme

In our experience some additional nodes are often found by the scan.
What is worse, SSH and other usual ports may be available on them.

```
# Nmap 7.80 scan initiated [redacted] as: /usr/bin/nmap -sT -n -Pn -vvv [redacted]
# Ports scanned: TCP(1000;1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,
Host: 10.[redacted].1 ()    Status: Up
Host: 10.[redacted].1 ()    Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].129 ()  Status: Up
Host: 10.[redacted].129 ()  Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].161 ()  Status: Up
Host: 10.[redacted].161 ()  Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].186 ()  Status: Up
Host: 10.[redacted].186 ()  Ports: 5060/open/tcp//sip///    Ignored State: filtered (999)
Host: 10.[redacted].250 ()  Status: Up
Host: 10.[redacted].250 ()  Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].1 ()    Status: Up
Host: 10.[redacted].1 ()    Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].33 ()   Status: Up
Host: 10.[redacted].33 ()   Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].97 ()   Status: Up
Host: 10.[redacted].97 ()   Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].5 ()    Status: Up
Host: 10.[redacted].5 ()    Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6006/open/tcp//X11:6///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//htt
Host: 10.[redacted].35 ()   Status: Up
Host: 10.[redacted].35 ()   Ports: 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 8000/open/tcp//http-alt///
Host: 10.[redacted].37 ()   Status: Up
Host: 10.[redacted].37 ()   Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 8000/open/tcp//http-alt///, 8001/open/tcp//vcom-tunnel///
Host: 10.[redacted].41 ()   Status: Up
Host: 10.[redacted].41 ()   Ports: 6000/open/tcp//X11///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//http-alt///, 8099/open/tcp//unknown///
Host: 10.[redacted].61 ()   Status: Up
Host: 10.[redacted].61 ()   Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6006/open/tcp//X11:6///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//htt
Host: 10.[redacted].63 ()   Status: Up
Host: 10.[redacted].63 ()   Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//http-alt///, 8001/open/tcp/
Host: 10.[redacted].69 ()   Status: Up
Host: 10.[redacted].69 ()   Ports: 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//http-alt///
# Nmap done at [redacted]
```

Figure 8: Open SSH, X11, FTP and web-management ports

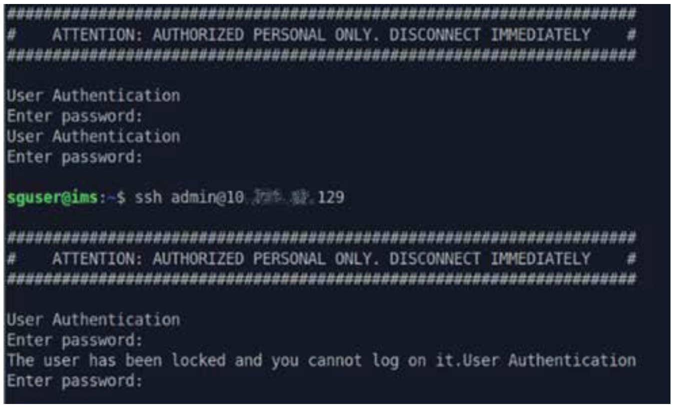


Figure 9: Locking the password for admin user via SSH

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 another 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.

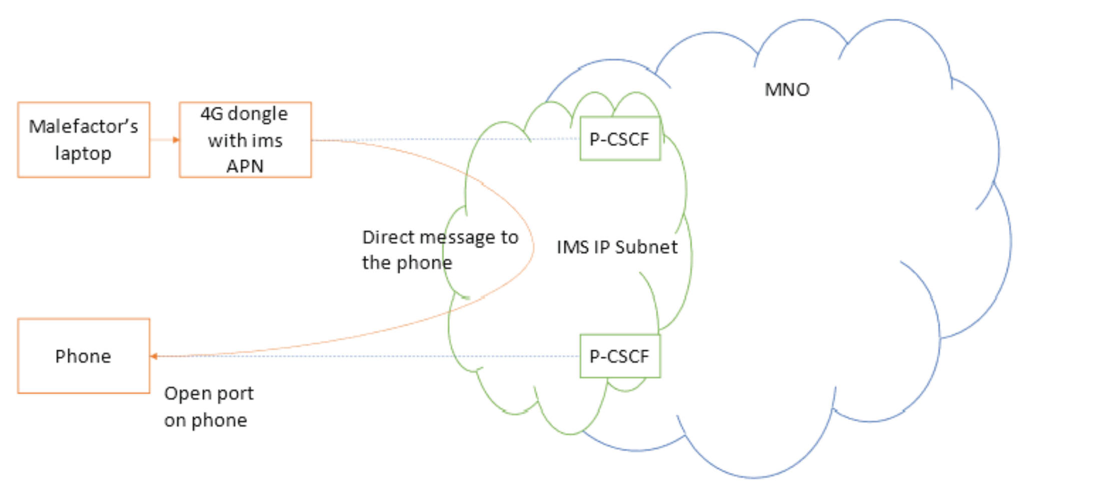


Figure 10: direct messaging attack scheme

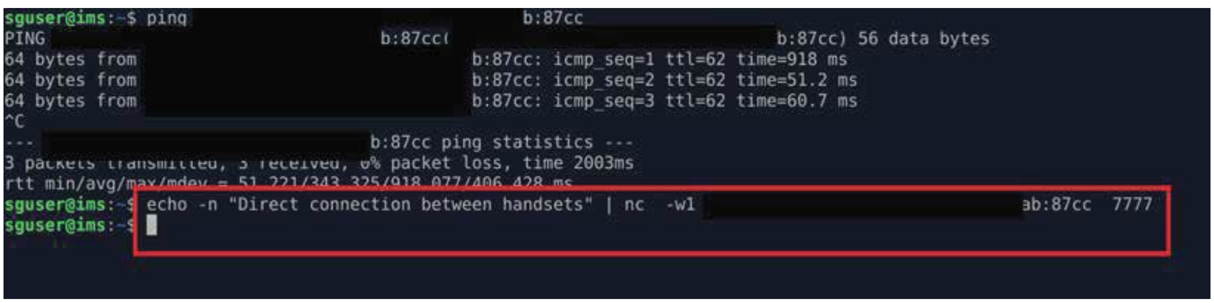


Figure 11: Direct communication with a phone, laptop side

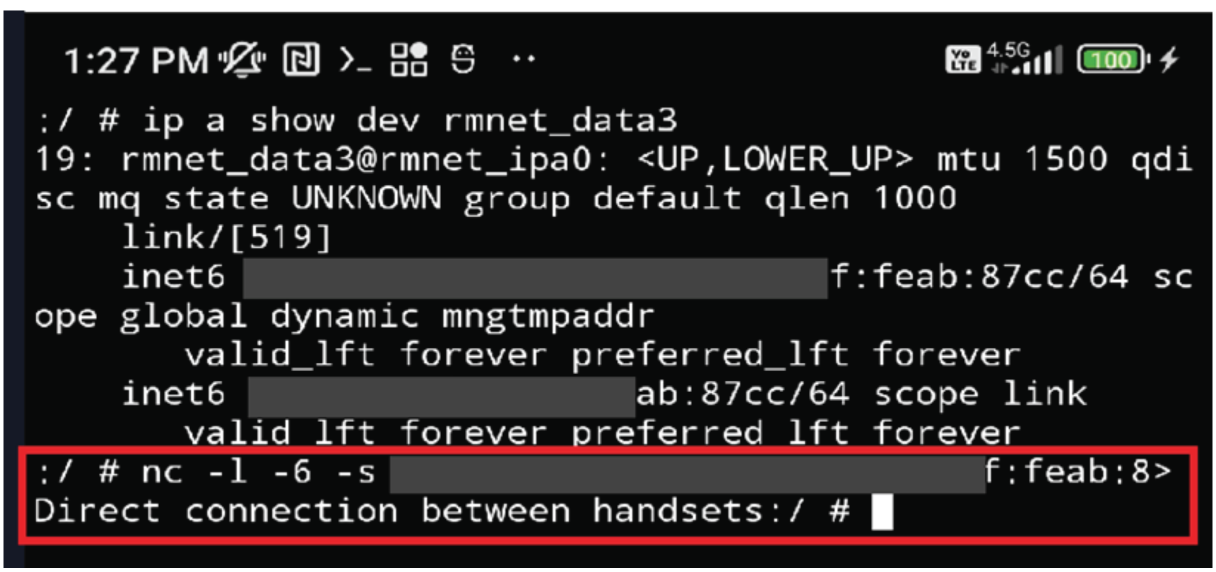


Figure 12: Direct communication with a phone, phone side

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.

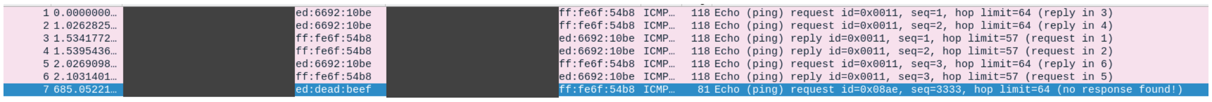


Figure 13. Ping with spoofed IP sent from PC.

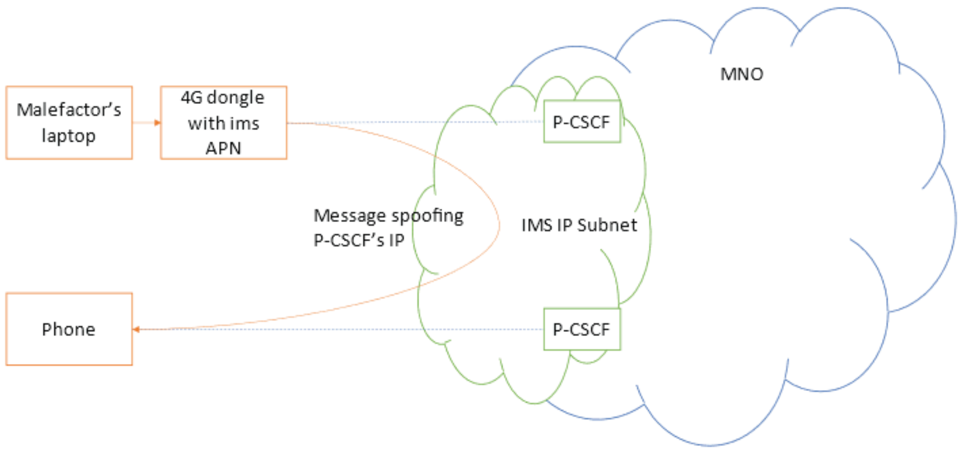


Figure 14: ip spoofing scheme

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 encryp tion 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 sub scriber'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 eaves-dropping.

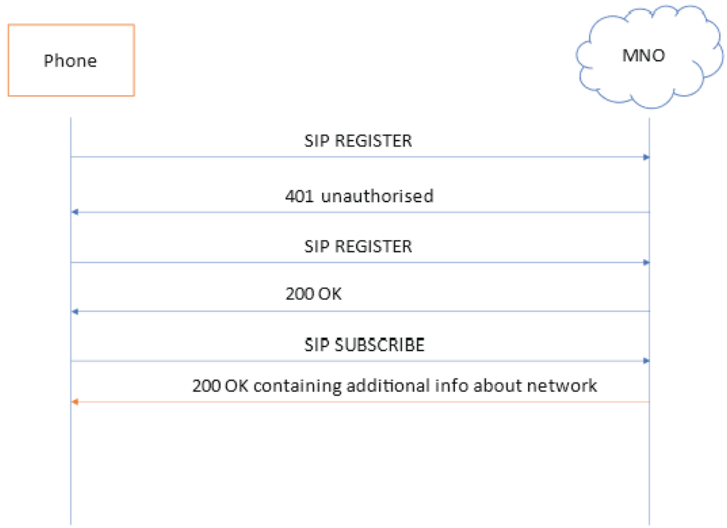
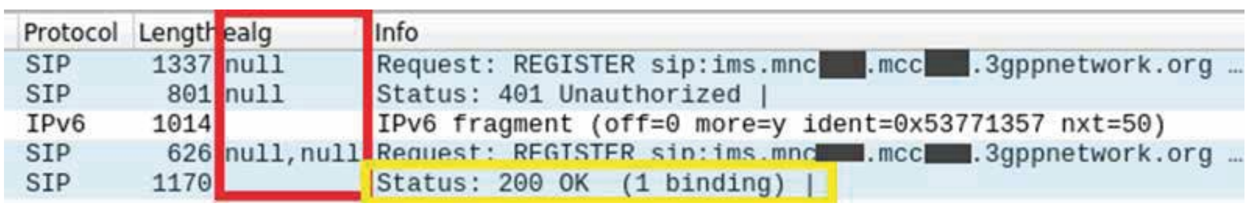
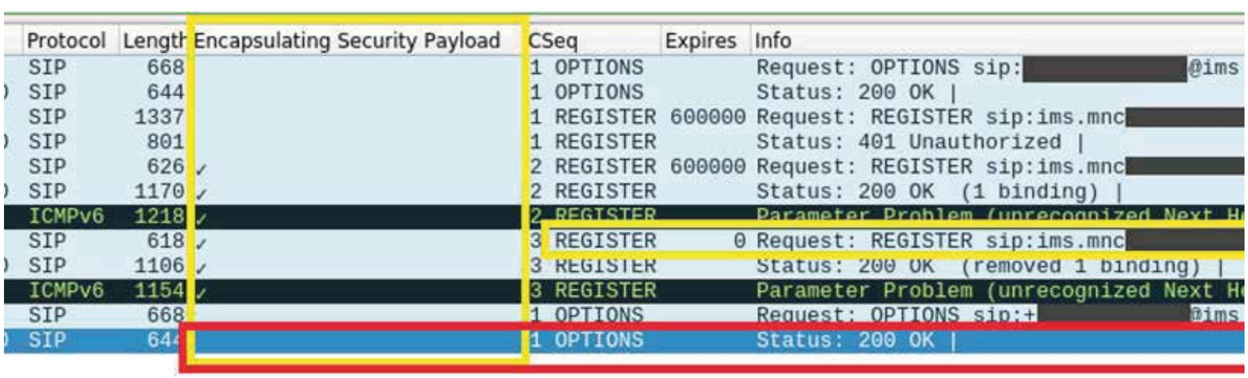


Figure 16. SIP REGISTER without IPSec scheme



Protocol	Length	ealg	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 REGISTER	600000	Request: REGISTER sip:ims.mnc[redacted]
SIP	801		1 REGISTER		Status: 401 Unauthorized |
SIP	626	✓	2 REGISTER	600000	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 REGISTER	0	Request: REGISTER sip:ims.mnc[redacted]
SIP	1106	✓	3 REGISTER		Status: 200 OK (removed 1 binding) |
ICMPv6	1154	✓	3 REGISTER		Parameter Problem (unrecognized Next He
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.

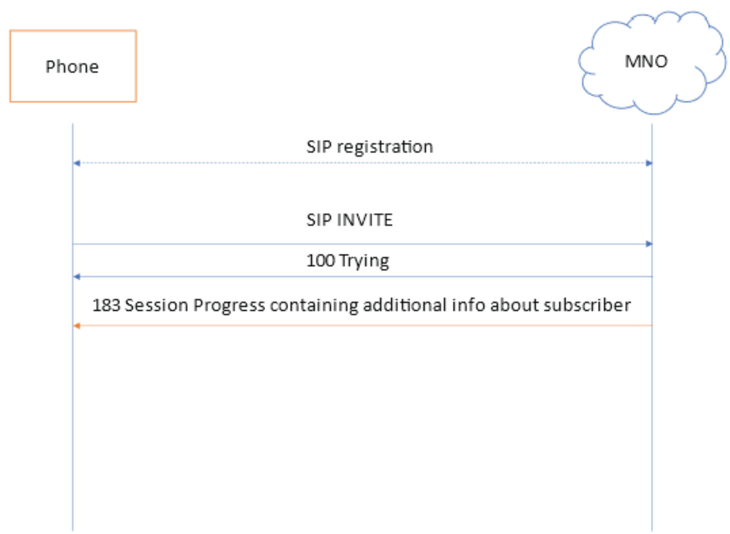


Figure 19. Disclosure of UE model scheme

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.

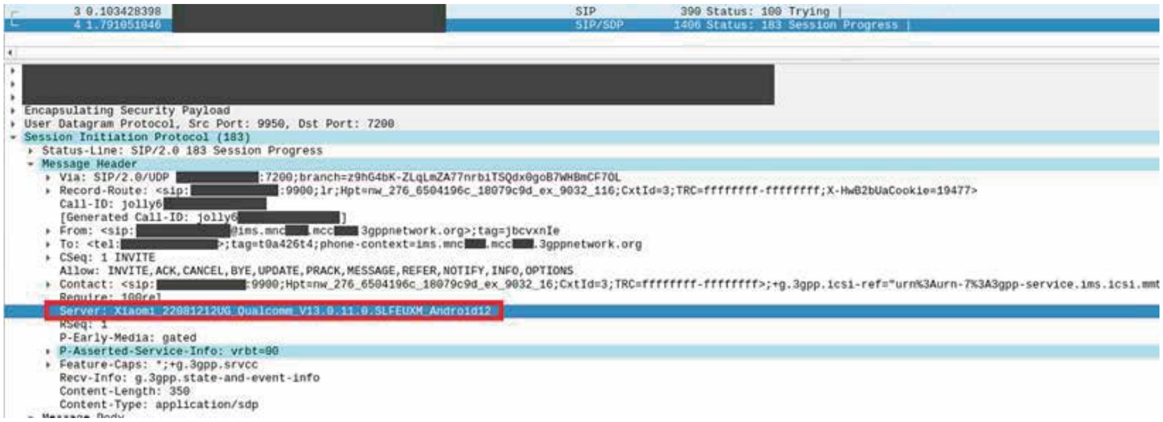


Figure 20. Disclosure of UE model

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

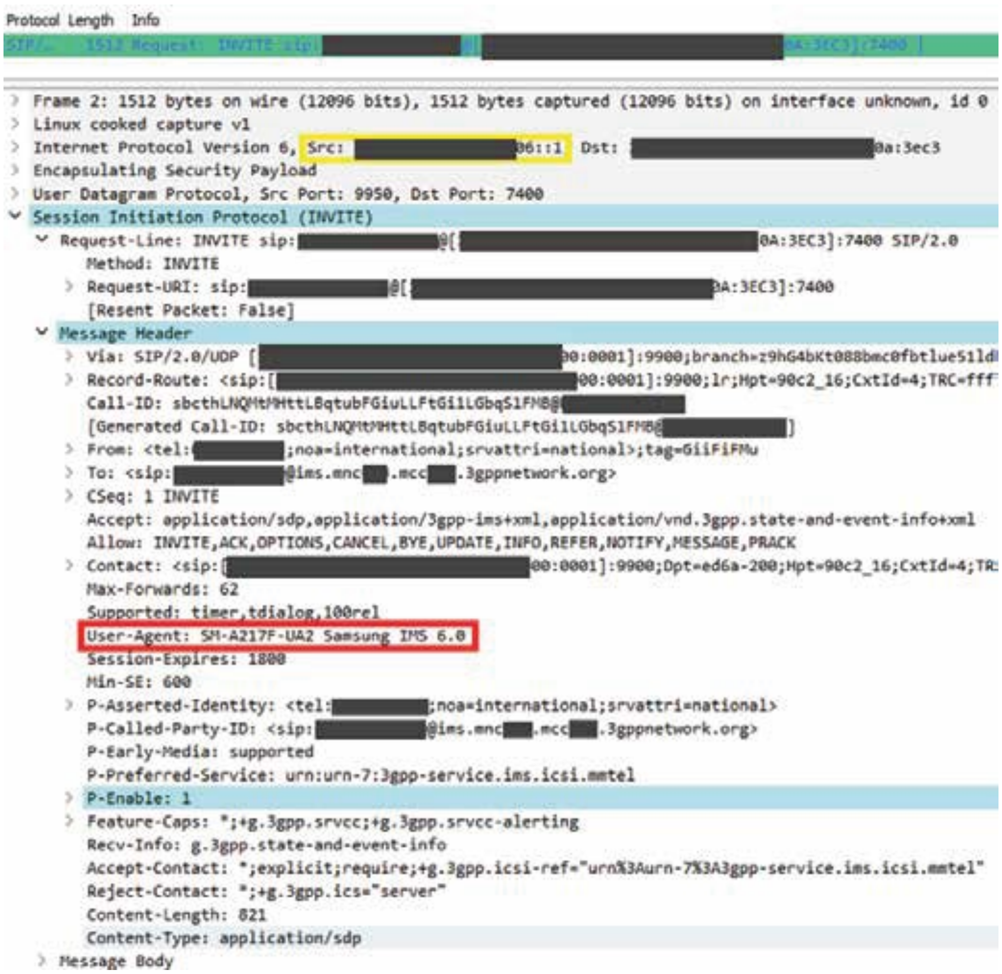


Figure 21. Subscriber user-agent disclosure

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

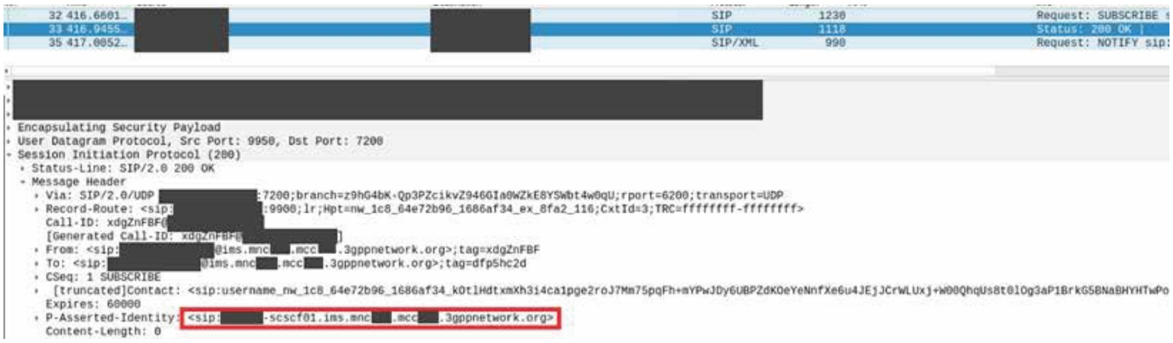


Figure 22: Disclosure of DNS names

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.

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.

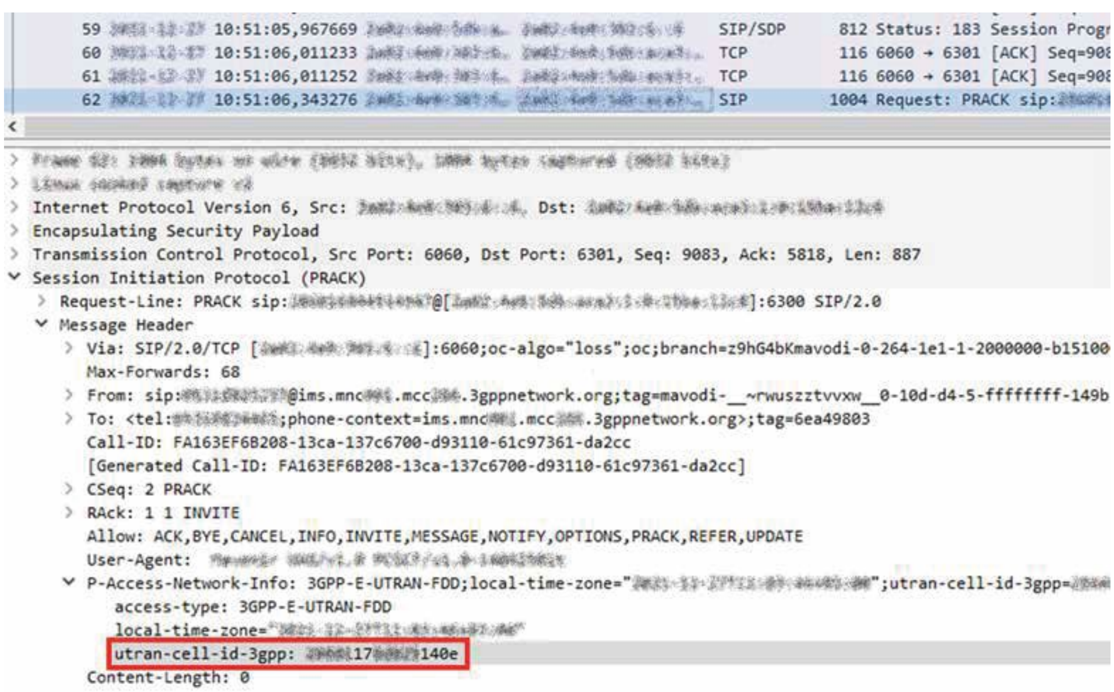


Figure 24. Location disclosure

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.

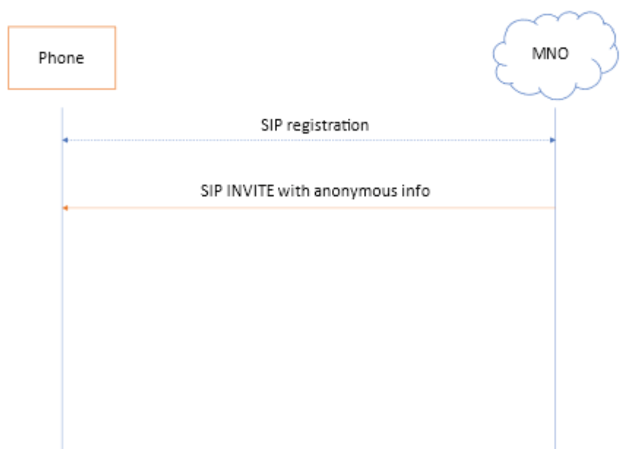


Figure 25. Subscriber info in anonymous call scheme

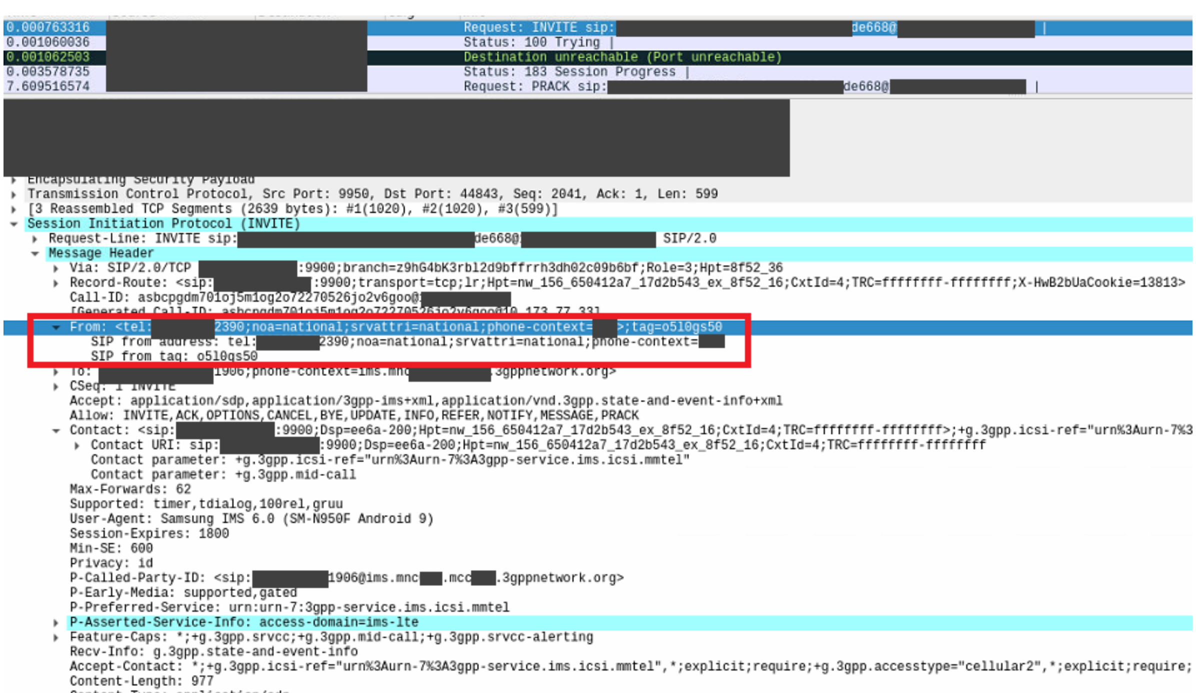


Figure 26. Subscriber info in anonymous call

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.**

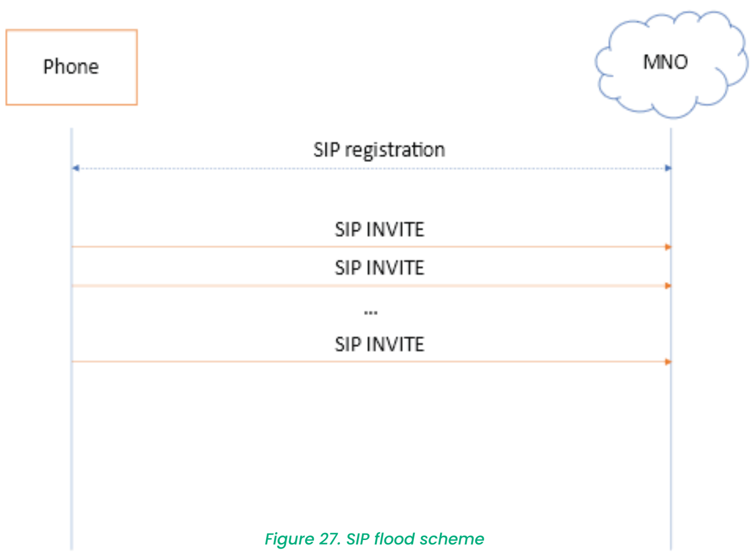
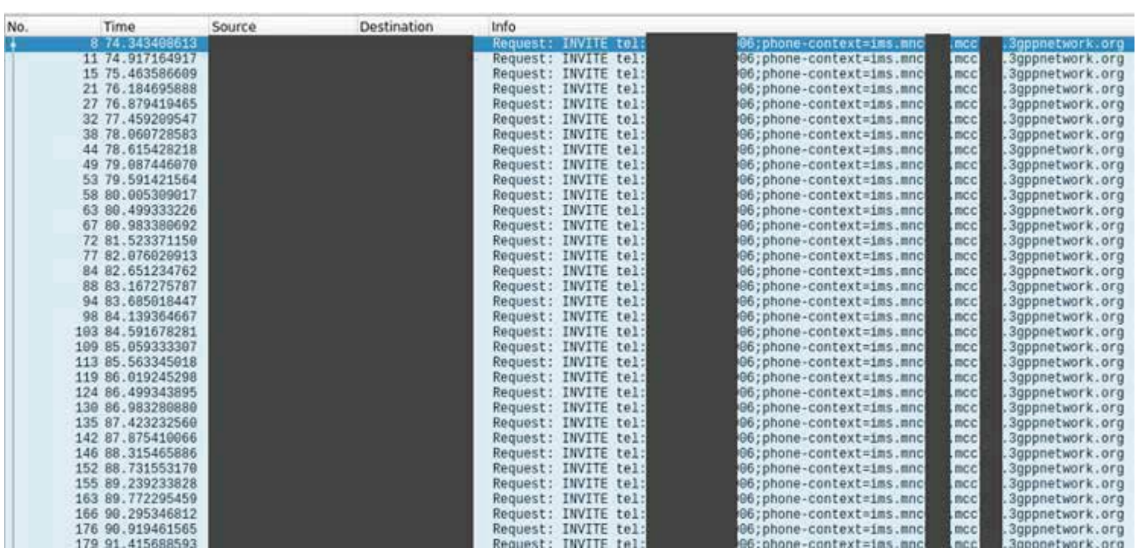


Figure 27. SIP flood scheme



No.	Time	Source	Destination	Info
8	74.343408613	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
11	74.917164917	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
15	75.463586609	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
21	76.184695888	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
27	76.879419465	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
32	77.459209547	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
38	78.060728583	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
44	78.615428218	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
49	79.087446070	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
53	79.591421564	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
58	80.005309017	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
63	80.499333226	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
67	80.983380692	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
72	81.523371150	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
77	82.076020913	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
84	82.651234762	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
88	83.167275787	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
94	83.685018447	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
98	84.139364667	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
103	84.591678281	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
109	85.059333307	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
113	85.563345018	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
119	86.019245298	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
124	86.499343895	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
130	86.983280880	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
135	87.423232560	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
142	87.875410066	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
146	88.315465886	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
152	88.731553170	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
155	89.239233828	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
163	89.772295459	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
166	90.295346812	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
176	90.919461565	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org
179	91.415688593	[redacted]	[redacted]	Request: INVITE tel:[redacted]06;phone-context=ims.mnc[redacted].mcc[redacted].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.

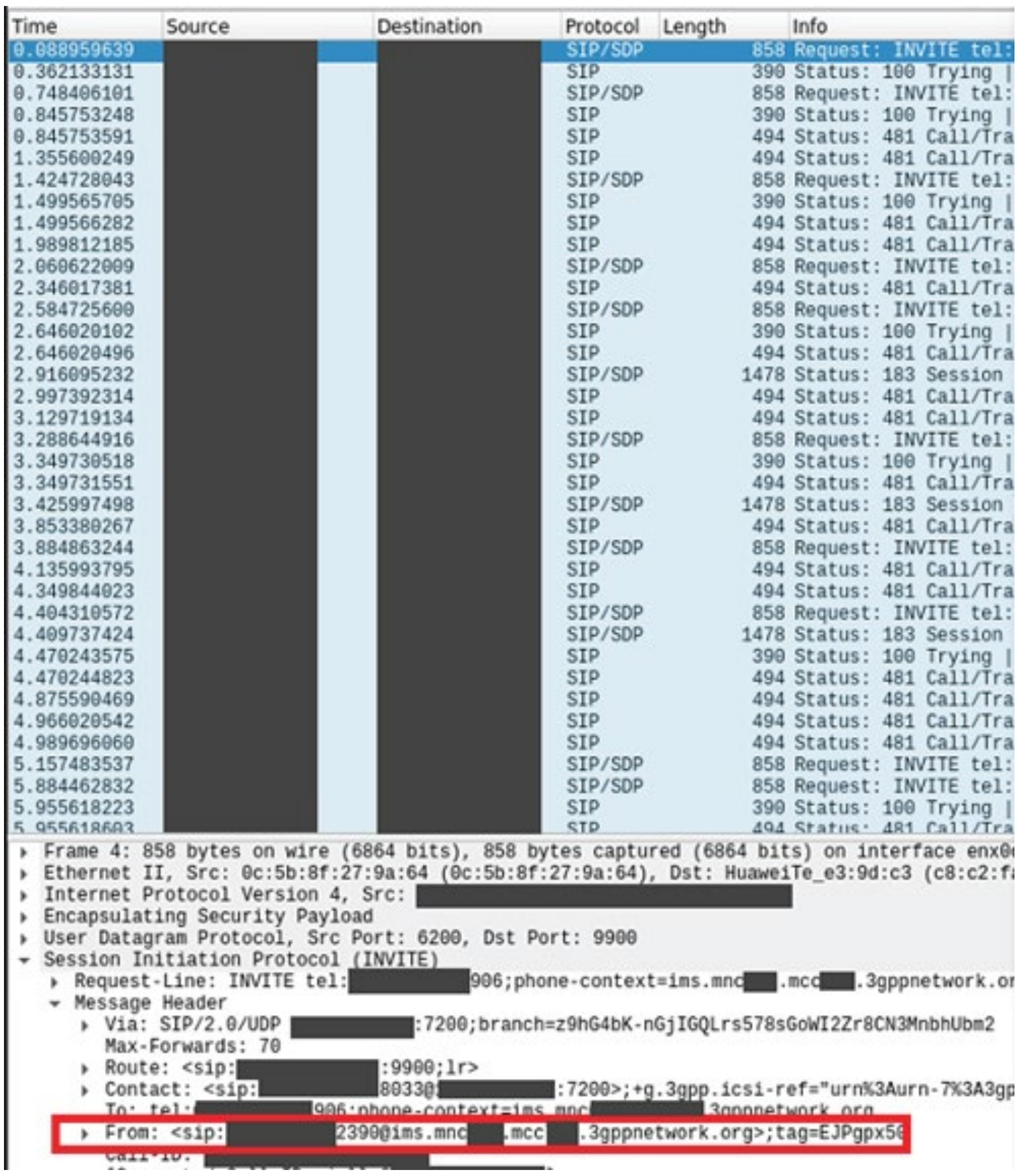


Figure 29. Subscriber DoS via SIP flood, attacker's side

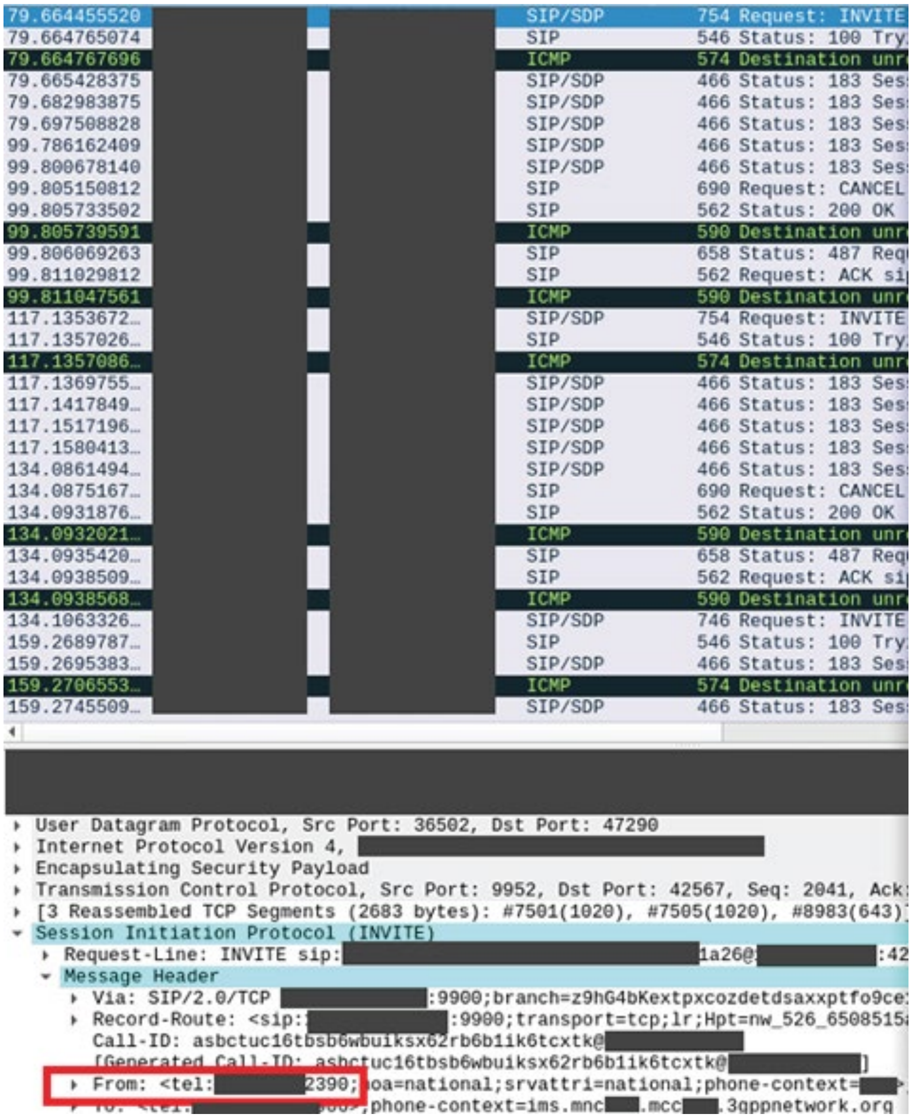


Figure 30: Subscriber DoS via SIP flood, victim's side

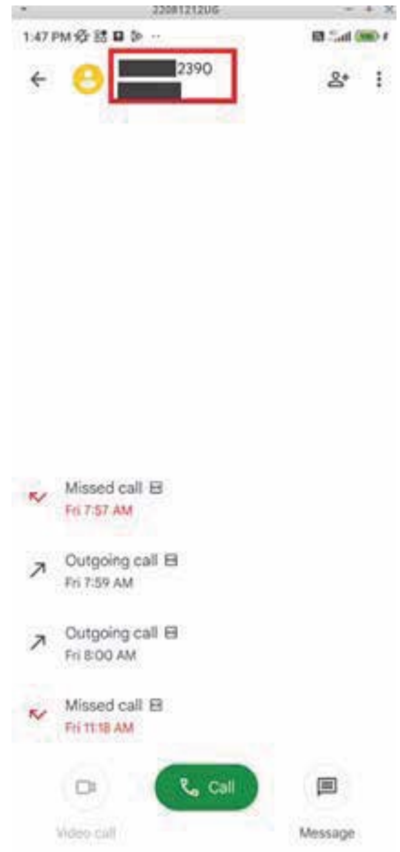


Figure 31: Subscriber DoS via SIP flood, phone with just a handful of missed calls during all this time.

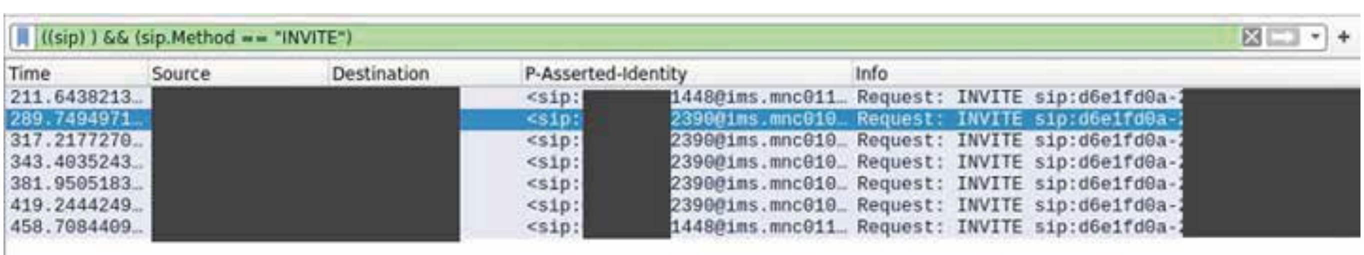


Figure 32: INVITEs from other phones are not routed while messages are being sent by malefactor

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.**

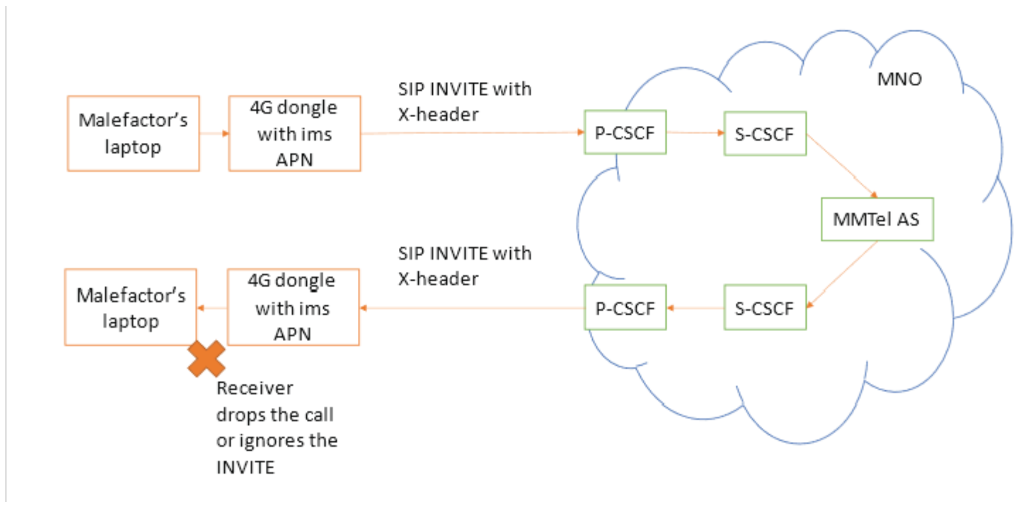


Figure 33: Sending unbilled data in INVITE scheme (1)

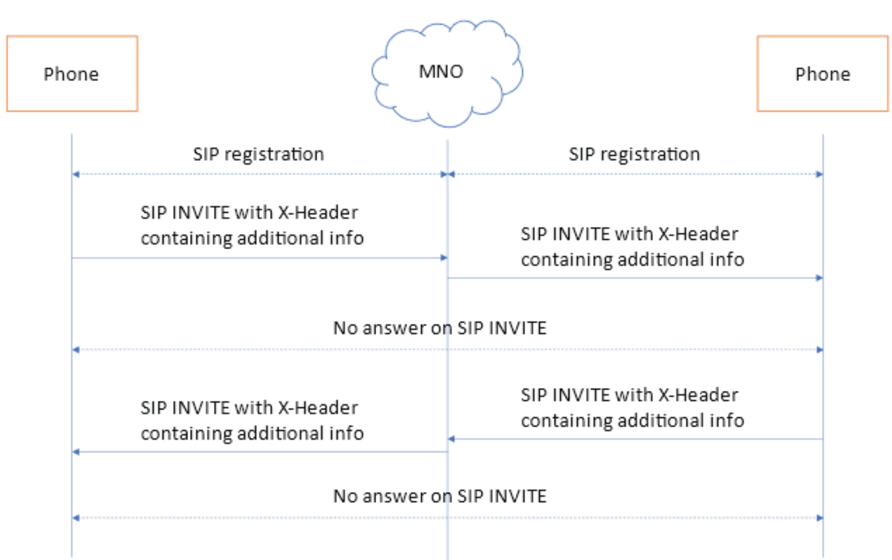


Figure 34: Sending unbilled data in INVITE scheme (2)

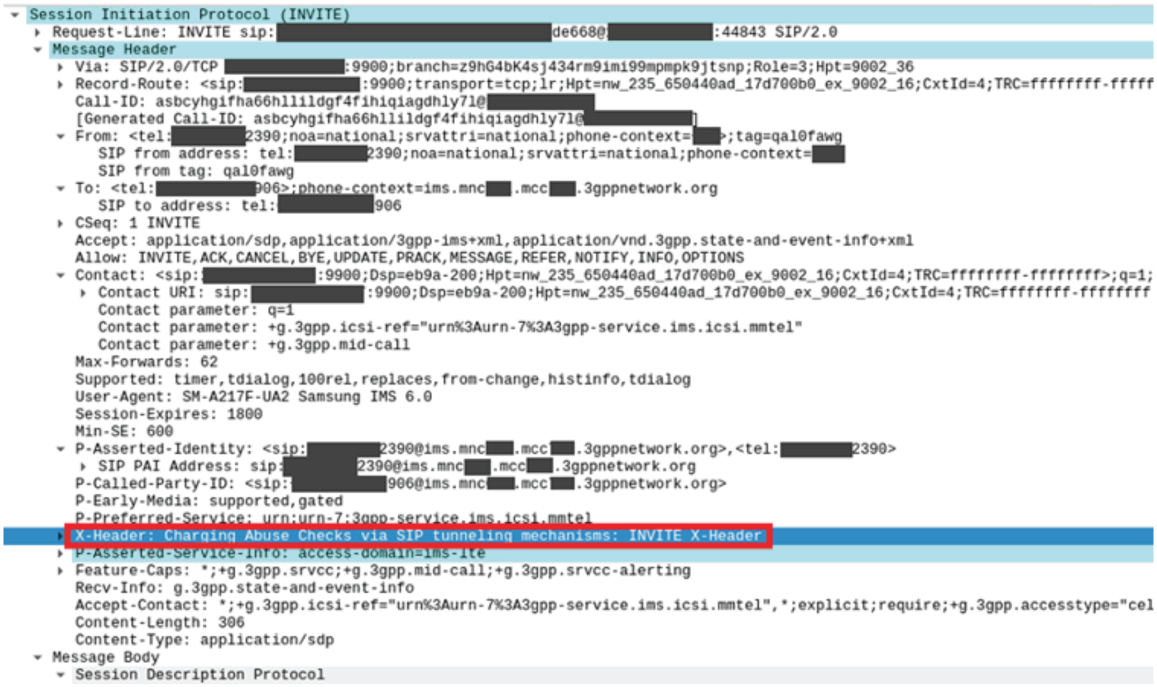


Figure 35. Sending unbilled data in INVITE

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.

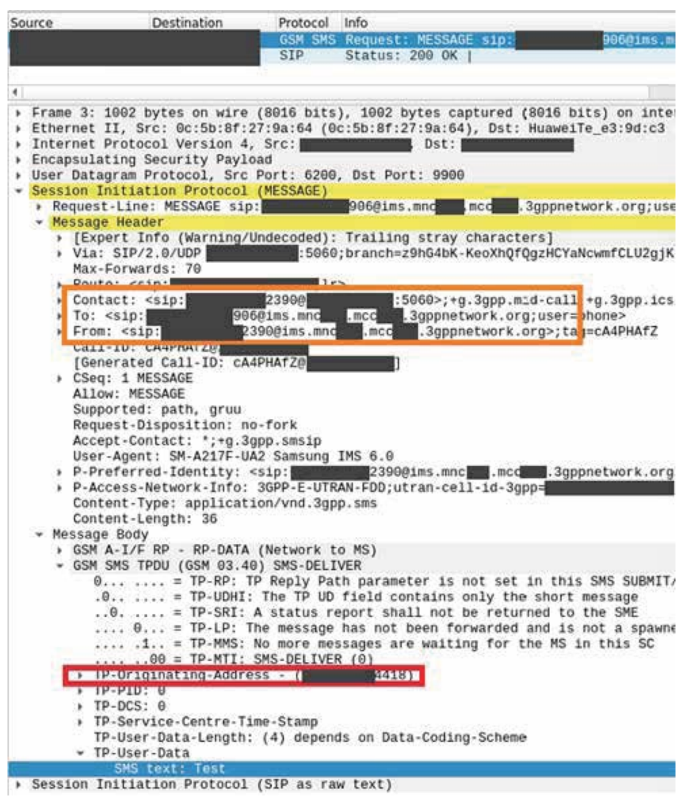


Figure 36: Spoofing source in MT SMS attacker's side

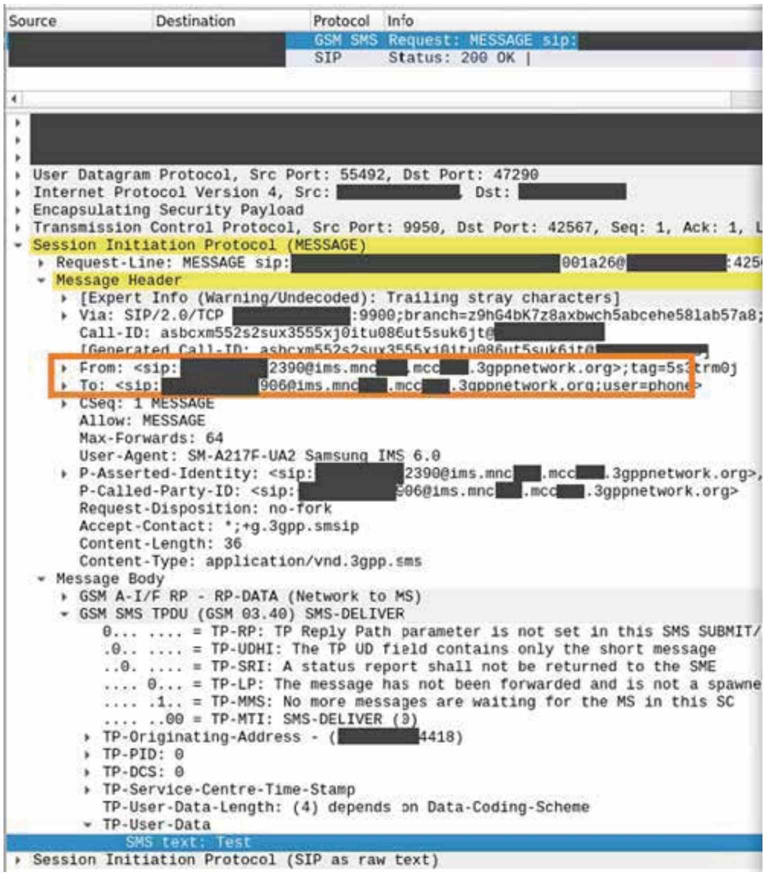


Figure 37: Spoofing source in MT SMS victim's side

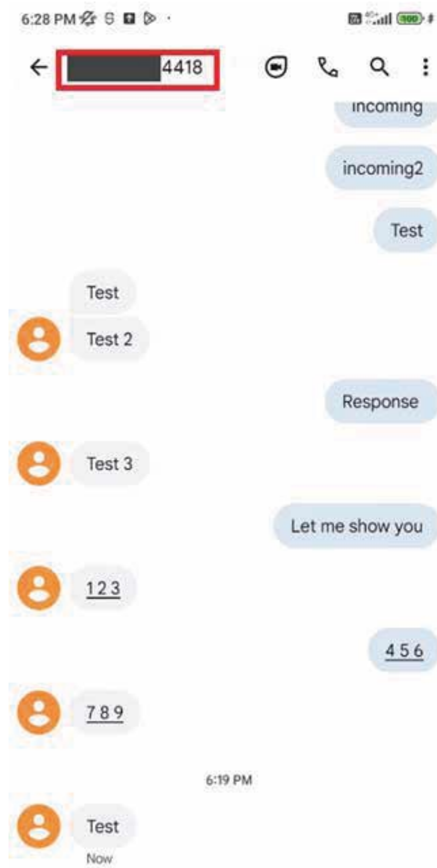


Figure 38: Spoofing source in MT SMS phone

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 capabili ties but also brings new security challenges. Operators must adopt a proactive approach to security, implementing robust encryption, secure network architec - ture, 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
GSMA	-	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
PGW	-	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