ERNW
providing security.

ERNW WHITE PAPER 60/ (SEPTEMBER, 2017)

PRACTICAL ATTACKS ON VOLTE AND VOWIFI

Version:	1.0
Date:	July 6, 2017
Author(s):	Sreepriya Chalakkal
Guide(s) :	Hendrik Schmidt, Shinjo Park

ERNW Enno Rey Netzwerke GmbH
Carl-Bosch-Str. 4
69115 Heidelberg

www.ernw.de
www.troopers.de
www.insinuator.net

Nichole Vonderwell

Digitally signed by Nichole Vonderwell
DN: c=DE, o=ERNW Insight GmbH, cn=Nichole Vonderwell, givenName=Nichole Christine, sn=Vonderwell, serialNumber=DTRWM741237304264922
Date: 2017.09.04 13:56:39 +02'00'

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Abstract

Voice over LTE (VoLTE) as well as Voice over WiFi (VoWiFi) are variants of Voice over IP that makes use of IP Multimedia Subsystem (IMS) in its backend. In this paper, we identify five different attacks on VoLTE/VoWiFi. This includes mainly (i)sniffing VoLTE/VoWiFi interfaces, (ii)extracting IPSec keys from IP Multimedia Services Identity Module (ISIM) that is embedded within the SIM card, and (iii)performing three different kinds of injection attacks in Session Initiation Protocol (SIP) headers that are used for signaling of VoLTE/VoWiFi. As a result of VoLTE/VoWiFi sniffing, we identified information disclosures such as leaking IMSI, IMEI, location of users and private IP of IMS. We also managed to extract the ciphering key and the integrity key (CK/IK) used for IPSec from ISIM with the help of a hardware device called SIMTrace [1]. We also discuss three different SIP header injection attacks that enables location manipulation and side channel attacks. It is important to note here that all these attacks are valid on the current 3GPP standards that are used by telecom providers. Thus, understanding the attacks and mitigating them is of high relevance.

2 Introduction

The evolution of telephony from public switched telephone network (PSTN) into delivering voice over Internet protocol (VoIP) has opened a new dimension for the provisioning of telephonic communication. This enabled making calls or sending SMS over 3G/4G or Wi-Fi. The digital information (voice and text), instead of being transmitted over a circuit-switched network, is packetized, and is transmitted as IP packets over a packet-switched network. Internet Protocol Multimedia Subsystem (IMS) is an architectural framework for IP based multimedia services. Voice over LTE (VoLTE) as well as Voice over WiFi (VoWiFi) are two variants of VoIP based services. SK Telecom and LG U+ is the first provider who introduced VoLTE in South Korea in 2012 [2]. Our tests were performed in Germany. Vodafone Germany is the first German operator to initiate the roll out of VoLTE in March 2015. On the other hand, Telekom introduced VoWiFi in Germany in May 2016. Both VoLTE as well as VoWiFi are very recent technologies and from a security perspective, they are not deeply understood or analyzed. In this paper, we perform a detailed security analysis of VoLTE and VoWiFi, with main focus on the communication channel between the User Equipment (UE) and the IMS. Figure 1 gives the overall architecture of systems involved. VoLTE falls in the 3GPP trusted network category as the access network is rather trusted by the provider. VoWiFi makes use of an untrusted WiFi access point and is thus always protected with an encrypted tunnel such as IPSec making use of Internet Key Exchange protocol (IKEv2) for initial Security Association establishment. The end point that handles tunnel authentication and authorization is called evolved packet data gateway (epdg).

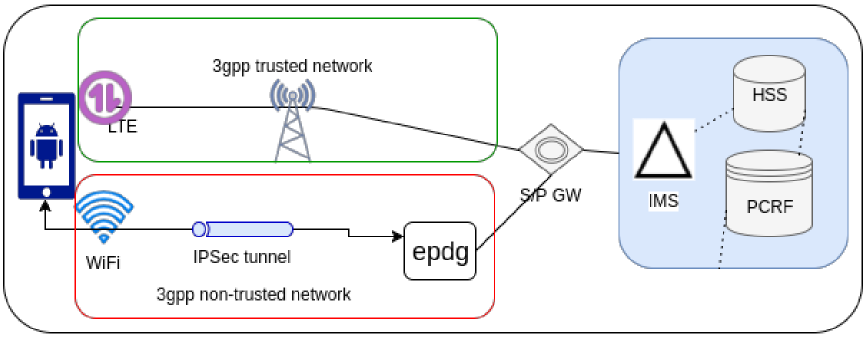


Figure 1 : Overall Architecture

Contributions: We present five new attacks on VoWiFi/VoLTE. The first one is about sniffing the VoLTE/VoWiFi interfaces and identifying information disclosures such as IMSI, IMEI, private IPs of IMS and location information. The second attack is focused on extracting the IPSec keys generated by the ISIM module embedded within the SIM card. We used the device SIMTrace [1] to sniff the ISIM traffic and implemented a Wireshark dissector to decode CK/IK found in ISIM.

The last three attacks are about performing SIP header injection that allows an attacker to perform spoofing, location manipulation and side channel attacks.

Terminology: In this paper, the attacks are common to both VoLTE and VoWiFi unless specified otherwise. Some important abbreviations used throughout the paper are as follows: UE (User Equipment (the mobile phone)), IMS (IP Multimedia Subsystem), SIP (Session Initiation Protocol used for signaling the voice traffic), ISIM (IP Multimedia Services Identity Module, an application within the SIM card responsible for generating the session keys for IPSec).

The remainder of this paper structures is as follows: In Section 3 , we discuss related work. Section 4 provides background information. Section 5 describes five different attacks on VoLTE/VoWiFi and the outcome is mentioned in Section 6. We present some mitigation in Section 7 and finally, Section 8 concludes our discussion.

3 Related Work

We categorize related works into three categories namely: VoWiFi attacks, VoLTE attacks and SIP attacks.

VoWiFi attacks: O'Hanlon et al. [3] talks about WiFi based IMSI catcher, which uses rogue WiFi access point to obtain the private identity of nearby users. In [4], O'Hanlon et al. further performs formal analysis on the security protocols EAP-AKA/SIM and provides PoC for IMSI catcher attacks. However, the prime focus here is mainly on attacking the UE. In this paper, we target the IMS rather than the UE. Our focus is to obtain the session keys for breaking the IPSec tunnel and the attacker is the UE. However, the information disclosures we identified such as IMSI and location information can be exploited by a rogue WIFI access point as mentioned in [3].

VoLTE attacks: The attacks mainly include free data channel, DoS and side-channel attacks on the IMS. Li et al. [5] presents two types of attacks. The first one is about establishing a free data service by sending each packet that gets forwarded from 4G gateway directly to the Internet. The second attack is a DoS attack that requires a malicious app (with no root privilege) to be installed on the victim device. This app performs DoS through the signaling bearer in VoLTE to the victims. Tu et al. [6] also describe another DoS attack where attacker makes 50 consequent VoLTE calls and hangs up before a SIP update is sent to VoLTE gateway by the caller. This attack leads to over power consumption causing power drainage at the receiver end. Kim et al. [7] mainly focus on side channel attacks to bypass IMS and also about permission mismatch issues in android VoLTE telephony apps.

SIP attacks: Fatih Ozavci [8] presents attacks targeting the IMS using SIP desktop client such as Skype business and Boghe IMS client. The attacks include fake software updates, injected XSS, bogus content types, fuzzing and eavesdropping attacks. Viproy toolkit [9], a metasploit framework is a useful tool for testing SIP injection attacks for desktop clients. Ahmad Abolhadid [10] also presents some attacks focusing on IMS that includes a variety of attacks such as spoofing, DoS and location manipulation. The last three attacks in our paper are mainly focused on SIP header injection. However, our attacks are in the context of VoLTE and VoWiFi based on our analysis.

All the attacks related to SIP and VoLTE are performed in an environment without any IPSec protection in place. There is also no authentication on integrity checks in any of these attacks. Hendrik et al. [11] presents a theoretical proposal of using SIMTrace hardware for extracting IPSec keys and performing SIP header injection for attacking the IMS. Our paper performs a practical implementation and partial validation of this idea.

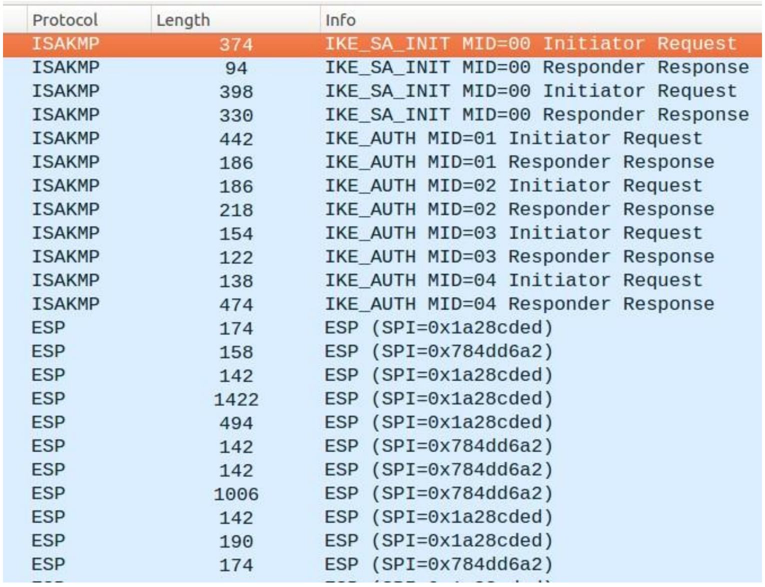
4 Background

In this section, we discuss about the security protocols involved in communication between UE and IMS. We also consider ISIM (IP Multimedia Services Identity Module) that resides in the SIM card. This contains the parameters for identifying the user, authenticating the user to the home network and for generating the session keys for IPSec. We also describe in detail about the IMS core and its major components, which is used for both VoWiFi and VoLTE call session.

4.1 Security Protocols

As shown in Figure 1, VoLTE uses the 3GPP trusted path and VoWiFi uses 3GPP non-trusted path for interacting with the IMS. In case of VoLTE, even though encryp- tion is recommended, it is not mandatory as defined in 3GPP TS 133.203. However, the user is registered to the home network using a variant of AKA protocol and the signaling and voice traffic is encapsulated with IPSec integrity protection. VoWiFi uses EAP-AKA (Authentication and Key Agreement) [12] protocol for key derivation and authentication, and IPSec to provide confidentiality and integrity of the communication. IPSec is using IKE (Internet Key Exchange) protocol to establish the session key (version 2 in our analysis).

IKEv2 consists of two phases as shown in Figure 2: during first phase `IKE SA INIT` both sides are negotiating the ciphering suite and encrypted channel to carry out the second phase. The actuāl āūthentication is performed within second phase `IKE AUTH`.



Protocol	Length	Info
ISAKMP	374	IKE_SA_INIT MID=00 Initiator Request
ISAKMP	94	IKE_SA_INIT MID=00 Responder Response
ISAKMP	398	IKE_SA_INIT MID=00 Initiator Request
ISAKMP	330	IKE_SA_INIT MID=00 Responder Response
ISAKMP	442	IKE_AUTH MID=01 Initiator Request
ISAKMP	186	IKE_AUTH MID=01 Responder Response
ISAKMP	186	IKE_AUTH MID=02 Initiator Request
ISAKMP	218	IKE_AUTH MID=02 Responder Response
ISAKMP	154	IKE_AUTH MID=03 Initiator Request
ISAKMP	122	IKE_AUTH MID=03 Responder Response
ISAKMP	138	IKE_AUTH MID=04 Initiator Request
ISAKMP	474	IKE_AUTH MID=04 Responder Response
ESP	174	ESP (SPI=0x1a28cded)
ESP	158	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x1a28cded)
ESP	1422	ESP (SPI=0x1a28cded)
ESP	494	ESP (SPI=0x1a28cded)
ESP	142	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x784dd6a2)
ESP	1006	ESP (SPI=0x784dd6a2)
ESP	142	ESP (SPI=0x1a28cded)
ESP	190	ESP (SPI=0x1a28cded)
ESP	174	ESP (SPI=0x784dd6a2)

Figure 2: ISAKMP followed by ESP packets

EAP-AKA is an adaption of AKA to be used within the EAP authentication framework. The USIM card and HSS shares the common secret, and HSS will generate the authentication token (RAND and AUTN) upon request. Upon successful authentication both UE and IMS core will share the key derived by the given token, without actually sending the key over-the-air.

4.2 ISIM Authenticate

This is a command specified in 3GPP TS 31.103 [13] used for authenticating the SIM to its home network. Among different contexts mentioned in the specification, we consider the IMS AKA security context during the procedure for authenticating the ISIM to its home network and vice versa when IMS AKA authentication data are available. The function is used whenever an IMS context is established, i.e. when the terminal receives a challenge from the IMS. A cipher key (CK) and an integrity key (IK) are calculated based on the challenge received. The ISIM uses the subscriber authentication key K, which is stored in the ISIM for the calculation of session key. 3GPP TS 31.103 [13] describe in detail about the algorithm for calculation of the keys. Once the keys are successfully computed, they are sent as response packet to `GSM SIM AUTHENTICATION` request. This can be parsed to obtain the keys.

4.3 IP Multimedia Subsystem

Both VoLTE and VoWiFi is built based on the IMS, which is designed to be access technology (Wi-Fi, 4G, etc.) agnostic and provide multimedia services like voice and video call, rich communication [14]. IMS utilizes common IP-based protocols like SIP, RTP, IPSec, to allow any IP-enabled devices to utilize services provided by IMS securely and easily. In this paper, we use the term IMS to address access technology agnostic parts, and specific technology name like VoWiFi, VoLTE is only used to deal with the specific problem.

Each communication made within IMS network is called IMS session. Within the session, users are able to use a variety of services like voice and video calls, content sharing, and they are added or removed from the session on-the-fly. What kind of data, and the properties of data inside the communication session is determined by PCRF (Policy and Charging Rule). PCRF and UE negotiates communication parameters like media type, bitrate utilizing the SIP (Session Initiation Protocol) messages.

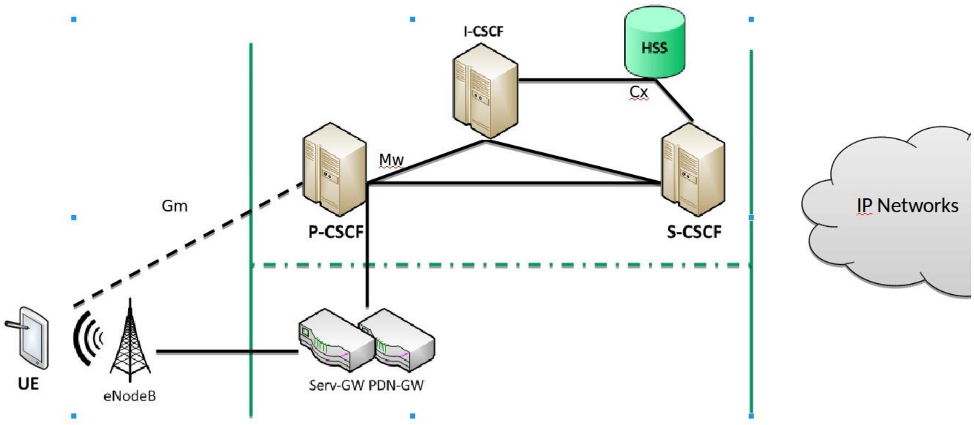


Figure 3: IMS Architecture

Figure 3 shows the overall architecture of IMS core network, containing the UE, CSCF, and other auxiliary entities. CSCFs (Call Session Control Function) are responsible for IMS session management and routing, and there are four different types of CSCF:

- Proxy call session control function (P-CSCF)
- Serving call session control function (S-CSCF)
- Interrogating call session control function (I-CSCF)
- Emergency call session control function (E-CSCF)

The first contact point of IMS-capable UE to the IMS core network is P-CSCF of the serving network. P-CSCF handles all signaling messages coming from UE, and routes it to the required nodes. P-CSCF is also responsible for applying integrity protection and ciphering the SIP signaling message, normally with IPSec or TLS.

Upon receiving registration request by P-CSCF, serving network's P-CSCF contacts the I-CSCF of the home network. I-CSCF then asks HSS about the legitimacy of the request and relays the authentication data if required. Upon successful authentication, S-CSCF of the home network will handle the IMS user. S-CSCF is in charge of routing the voice and video calls, and it also asks HSS (Home Subscriber Service) whether the requested service is available or not. HSS stores subscriber's data including private user identity, charging information and others. Finally, if the IMS core supports emergency services, calls to the services like police or ambulance will be handled by the dedicated E-CSCF.

5 Practical Attacks

This section explains in detail about five different attacks named from A1 to A5. The first attack A1 is about sniffing the VoLTE/VoWiFi interfaces of the UE during a variety of use cases such as IMS registration, incoming call and outgoing call. The second attack, A2 is listening to the ISIM interface within the USIM card of the user to obtain the IPSec keys. This attacks need the hardware device SIMTrace [1]. The last three attacks, A3, A4 and A5 are injection attacks performed on SIP headers for location manipulation and obtaining a side channel. But the attacks are performed in OpenIMS [15], which is an open source implementation of IMS. Even though OpenIMS is not used by major providers, the implementation follows 3GPP standard [15] which is the main standard for IMS implementation. Our pen testing experience with providers also confirms the possibility of such attacks. Hence, we argue that the attacks are equally relevant as in a real telecom provider network.

5.1 A1: Sniffing VoLTE/VoWiFi Interfaces

Setup : Table 1 lists the features (VoLTE/VoWiFi) supported by the test devices (Samsung S6 and S7). It is important to note here that there should be support from the provider as well as the phone in order to make a VoLTE/VoWiFi call. In order to sniff the VoLTE/VoWiFi traffic, we need to root the phone and also install tcpdump.

This attack involves listening to VoLTE interface (rmnet) and VoWiFi interface (wlan,epdg) and identify non-encrypted communication. Figure 5 shows the components and interface in case of VoLTE. This is a 3GPP trusted network. All the captures in association with VoLTE involves sniffing the interface rmnet1 (or rmnet0). There is IPSec in place for authentication. But there is no encryption. On the other hand, VoWiFi falls in the category of 3GPP non-trusted network. Hence the communication is via an IPSec tunnel in the interface wlan0. However, we identified a hidden virtual inter- face, named epdg1 that contains non-encrypted packets that are integrity protected using ESP (IPSec). In both the cases (VoLTE and VoWiFi), we used Wireshark compiled with Gcrypt to decode the ESP packets to get SIP and TCP packets embedded within.

```
# Sniffing VoLTE interface :
# rmnet is for VoLTE.
# Replace it with epdg/wlan0 for VoWiFi.
$ adb shell
$ tcpdump -i rmnet1 -n -s 0 -w - |
nc -l 127.0.0.1 -p 11233
$ adb forward tcp:11233 tcp:11233 &&
nc 127.0.0.1 11233 | wireshark -k -S -i -
```

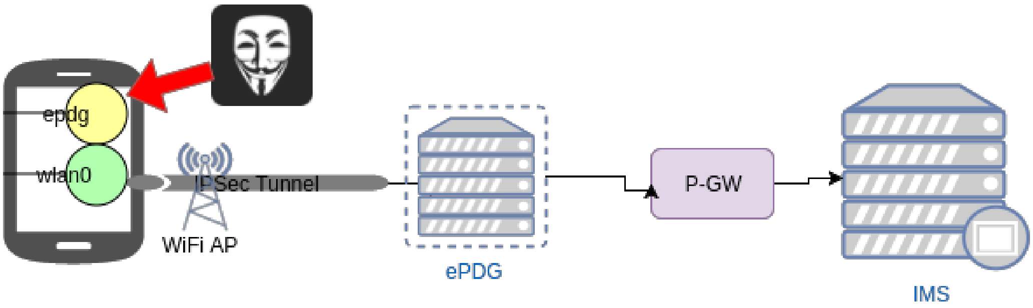


Figure 4: Sniffing VoWiFi from epdg1 virtual interface

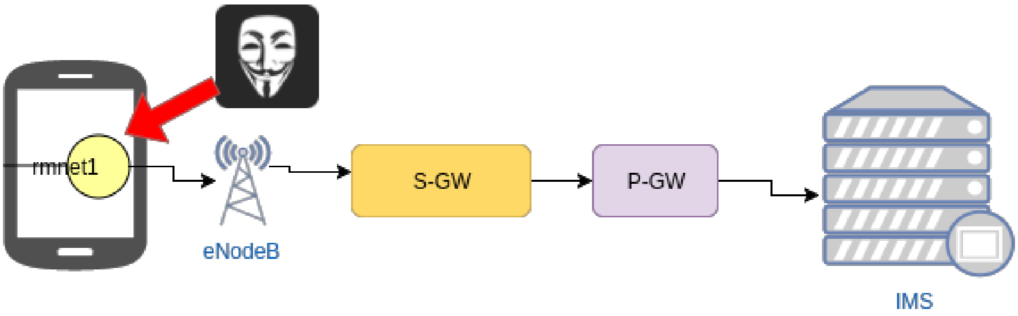


Figure 5: Sniffing VoLTE traffic from rmnet1 interface

5.2 A2: ISIM sniffing for extracting CK/IK

Setup: We performed sniffing in the ISIM interface of the SIM card in order to intercept the traffic between the ISIM and the phone. We make use of a hardware device called SIMTrace [1] as shown in Figure 7. We need to take the SIM card out of the phone and place it in SIMTrace and connect SIMTrace to the SIM slot of the phone.

ISIM is an application residing in the UICC (SIM card). ISIM stores IMS specific subscriber data. This data is mainly used during the initial user registration of the device to the IMS. Below are some of information that are stored in ISIM [14].

- Private user identity of the user - this is used in registration request to identify user's subscription.
- Security parameters - used for IMS authentication such as shared secret, sequence number.
- Address of P-CSCF - this can be used when the access technology does not support dynamic P-CSCF discovery capabilities.
- Entry point of home network - this is used in registration to route the request to user's home network.

All the information, except the security parameters (shared secret), are sent in the initial REGISTER request

Table 1: VoLTE/VoWiFi support in Telekom(T) and O2 in Samsung S6 and S7

Service	T. S6	T. S7	O2 S6	O2 S7
VoWiFi	Yes	No	No	No
VoLTE	Yes	Yes	No	Yes

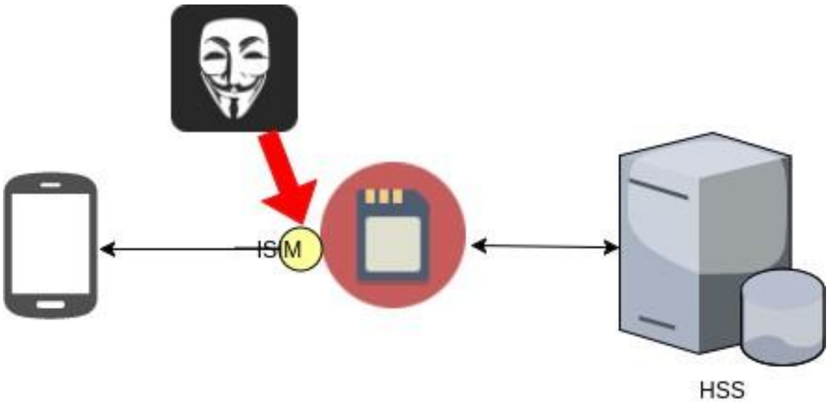


Figure 6: Sniffing ISIM traffic using SIMTrace

from the UE which can be sniffed with A1. We also noticed that, except for the initial REGISTER request, all other packets are integrity protected with IPSec. During the AKA transaction as mentioned in Section 3, the parameters for generation of IPSec keys are exchanged. The IPSec keys are generated in the ISIM within the UICC and are sent to the kernel when the IPSec client request them. To extract these keys, we performed the attack as shown in Figure 6 using SIMTrace.

Table 2: Parsing the ISIM Authenticate response to get IK and CK

Byte(s)	Description	Length
1	'Successful 3G authentication' tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5

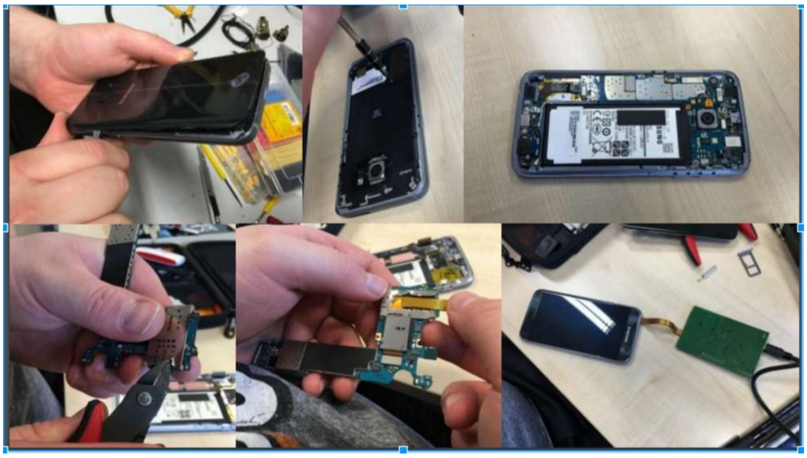
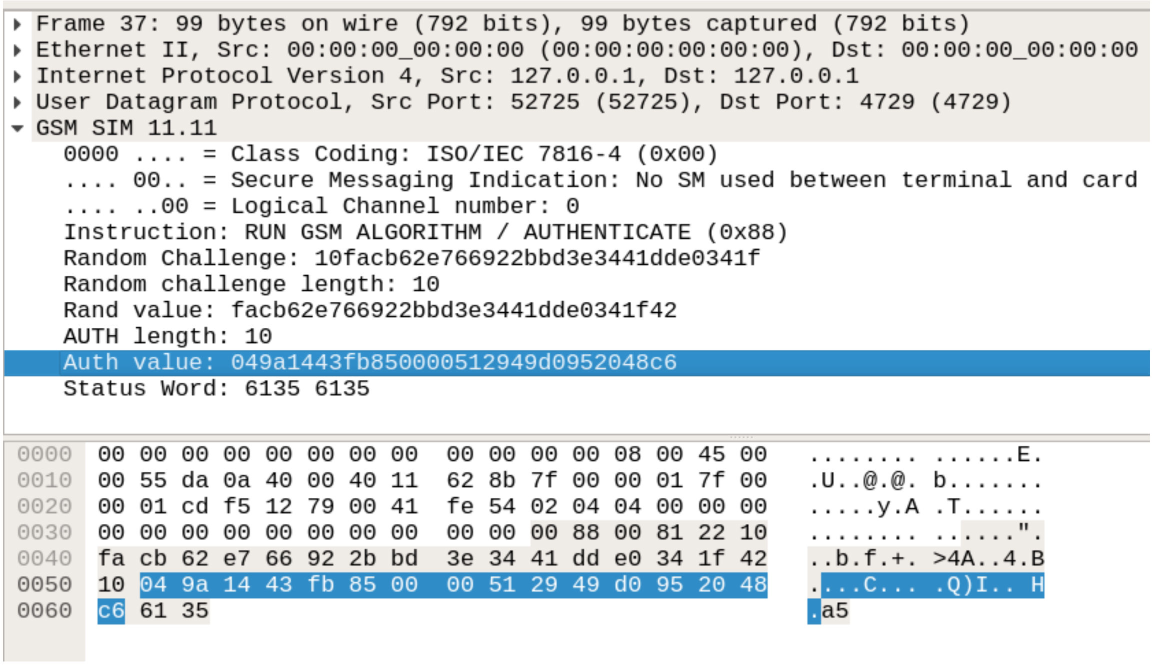


Figure 7: SIMTrace with Samsung S7

The current compilation of Wireshark does not support dissection of the payload of the AKA packets as seen as `GSM AUTHENTICATE` and `GSM RESPONSE` in wireshark. This can be parsed by following the documentation in TS 31.103 [13] as explained in Table 2.



```
▸ Frame 37: 99 bytes on wire (792 bits), 99 bytes captured (792 bits)
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ User Datagram Protocol, Src Port: 52725 (52725), Dst Port: 4729 (4729)
▾ GSM SIM 11.11
    0000 .... = Class Coding: ISO/IEC 7816-4 (0x00)
    .... 00.. = Secure Messaging Indication: No SM used between terminal and card
    .... ..00 = Logical Channel number: 0
    Instruction: RUN GSM ALGORITHM / AUTHENTICATE (0x88)
    Random Challenge: 10facb62e766922bbd3e3441dde0341f
    Random challenge length: 10
    Rand value: facb62e766922bbd3e3441dde0341f42
    AUTH length: 10
    Auth value: 049a1443fb850000512949d0952048c6
    Status Word: 6135 6135

0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 55 da 0a 40 00 40 11  62 8b 7f 00 00 01 7f 00   .U..@.@. b.......
0020  00 01 cd f5 12 79 00 41  fe 54 02 04 04 00 00 00   .....y.A .T......
0030  00 00 00 00 00 00 00 00  00 00 00 88 00 81 22 10   ........ ......".
0040  fa cb 62 e7 66 92 2b bd  3e 34 41 dd e0 34 1f 42   ..b.f.+. >4A..4.B
0050  10 04 9a 14 43 fb 85 00  00 51 29 49 d0 95 20 48   ....C... .Q)I.. H
0060  c6 61 35                                           .a5
```

Figure 8: Wireshark dissector for AUTN and RAND

5.3 A3: User location manipulation

Setup: The attack is performed in an experimental set up with OpenIMS as the backend. We use desktop SIP client to perform the test and SIP Proxy tool [16] for performing the injection. However, we argue that the attack is valid from a VoLTE/VoWiFi clients as well due to the fact that the 3GPP standardization does not include proper mitigation to such attacks. We are also able to confirm this with our experience of penetration testing with telecom providers.

`P-Access-Network-Info` is the header field in SIP that defines the user location in the access network [17]. If the access network is a mobile network (such as 3G or LTE), the header field contains information such as: Mobile Network Code (MNC), Mobile Country Code (MCC), Local Area Code (LAC) and Cell Identifier. Essentially, this header contains information on the access network that the UE is using to get IP connectivity. A special class of values are defined for use here, as the same granularity of values may not be possible as for those available from the UE: `3GPP-GERAN, 3GPP-UTRAN, 3GPP-WLAN, 3GPP-GAN, and 3GPP-HSPA.`

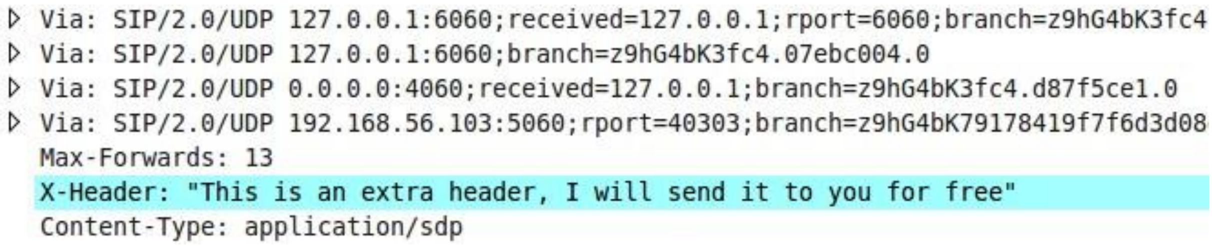
`P-Access-Network-Info` header field may contain an attribute called network-provided or np. It means that the P-CSCF is responsible to get the location of the user, because the access network does not enable the user to provide such information. So when a P-CSCF receives a SIP request from a user with a header containing np, it removes the header completely, fetches the location information (from any access network node) and adds a new `P-Access-Network-Info` header with the user lo- cation. However, if `P-Access-Network-Info` header does not contain np, P-CSCF trusts the location information provided by the user and does not double check it with the value in HSS.

5.4 A4: Roaming information manipulation

The setup for this attack is same as in A3. `P-Visited-Network-ID` is a header field in SIP packets that decides the access network that serves the user [17]. During registration of a user, P-CSCF populates this header field with a unique identity of the access network, and adds it to the REGISTER request. When S-CSCF receives this REGISTER request, it decides the access network of the user according to this header. So, in short, `P-Visited-Network-ID` decides if the user is roaming or not.

5.5 A5: Side channel attack

The setup for the attack is same as in A3.



```
▷ Via: SIP/2.0/UDP 127.0.0.1:6060;received=127.0.0.1;rport=6060;branch=z9hG4bK3fc4
▷ Via: SIP/2.0/UDP 127.0.0.1:6060;branch=z9hG4bK3fc4.07ebc004.0
▷ Via: SIP/2.0/UDP 0.0.0.0:4060;received=127.0.0.1;branch=z9hG4bK3fc4.d87f5ce1.0
▷ Via: SIP/2.0/UDP 192.168.56.103:5060;rport=40303;branch=z9hG4bK79178419f7f6d3d08
  Max-Forwards: 13
  X-Header: "This is an extra header, I will send it to you for free"
  Content-Type: application/sdp
```

Figure 9: Extra header field injection

SIP protocol is an extensible protocol. It allows networks or systems to add customized header fields to their SIP messages [18]. This feature can be misused by an attacker to exchange information in the header without being charged. They can populate information in additional header fields to uncharged SIP requests such as OPTIONS request. In [7], there is a mention about SIP tunneling attack where the attacker injects data in SIP header fields. This attack is very closely related to such an attack. SIP header injection is possible in other headers as well due to the lack of input validation in the server side. However, we identify the scenario of the use of the specific header called X-header (extensible header) that allows header injection.

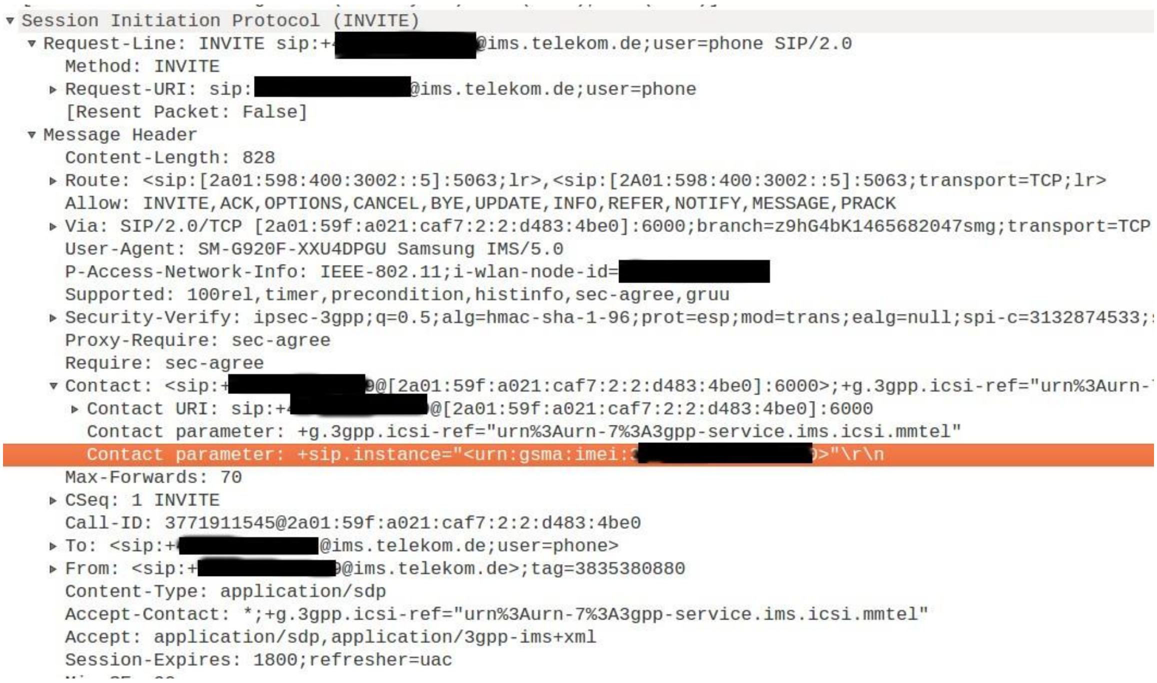
6 Results

This section contains the results of the attacks mentioned in previous section. The results are numbered in correspondence with the attack numbers.

6.1 R1: Information Disclosures

The sniffing attacks mentioned in A1 at VoLTE/VoWiFi interfaces resulted in some important information disclosures as mentioned in this section.

1. IMEI in `SIP REGISTER`: International Mobile Equipment Identity (IMEI) is the unique identification number for every mobile phones. IMEI is useful to identify if the device is barred (for e.g. if stolen by someone) before registering it. This is an intended usage. However, this is sent non-encrypted and without authentication (i.e. before any IPSec is set up) in `SIP REGISTER` as this is the first packet to the server before any security association is set up. Below is how we see it in `SIP REGISTER` in the Contact header:



```
▾ Session Initiation Protocol (INVITE)
  ▾ Request-Line: INVITE sip:+[redacted]@ims.telekom.de;user=phone SIP/2.0
      Method: INVITE
    ▸ Request-URI: sip:[redacted]@ims.telekom.de;user=phone
      [Resent Packet: False]
  ▾ Message Header
      Content-Length: 828
    ▸ Route: <sip:[2a01:598:400:3002::5]:5063;lr>,<sip:[2A01:598:400:3002::5]:5063;transport=TCP;lr>
      Allow: INVITE,ACK,OPTIONS,CANCEL,BYE,UPDATE,INFO,REFER,NOTIFY,MESSAGE,PRACK
    ▸ Via: SIP/2.0/TCP [2a01:59f:a021:caf7:2:2:d483:4be0]:6000;branch=z9hG4bK1465682047smg;transport=TCP
      User-Agent: SM-G920F-XXU4DPGU Samsung IMS/5.0
      P-Access-Network-Info: IEEE-802.11;i-wlan-node-id=[redacted]
      Supported: 100rel,timer,precondition,histinfo,sec-agree,gruu
    ▸ Security-Verify: ipsec-3gpp;q=0.5;alg=hmac-sha-1-96;prot=esp;mod=trans;ealg=null;spi-c=3132874533;
      Proxy-Require: sec-agree
      Require: sec-agree
    ▾ Contact: <sip:+[redacted]@[2a01:59f:a021:caf7:2:2:d483:4be0]:6000>;+g.3gpp.icsi-ref="urn%3Aurn-
      ▸ Contact URI: sip:+[redacted]@[2a01:59f:a021:caf7:2:2:d483:4be0]:6000
        Contact parameter: +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
        Contact parameter: +sip.instance="<urn:gsma:imei:[redacted]>"\r\n
      Max-Forwards: 70
    ▸ CSeq: 1 INVITE
      Call-ID: 3771911545@2a01:59f:a021:caf7:2:2:d483:4be0
    ▸ To: <sip:+[redacted]@ims.telekom.de;user=phone>
    ▸ From: <sip:+[redacted]@ims.telekom.de>;tag=3835380880
      Content-Type: application/sdp
      Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
      Accept: application/sdp,application/3gpp-ims+xml
      Session-Expires: 1800;refresher=uac
```

Figure 10: SIP Invite with information leaks

```
Contact:
<sip:262011202xxxxxx@[x.x.x.x]:6000>;
q=0.50;+g.3gpp.icsi-ref=
"urn%3Aurn-7%3A3gpp-service.ims.xxx";
+g.3gpp.smsip;+sip.instance= "<urn:gsma:imei:35490xxx-xxxxxx-0>"
```

2. **IMEI in `SIP INVITE`**: `SIP INVITE` consists of a parameter that contains the IMEI number of the caller. This is found in all the incoming calls in the header `Accept-Contact`.

```
Accept-Contact:
*;+sip.instance= "<urn:gsma:imei:354xxxxx7-xxxxxx-0>";
+g.3gpp.icsi-ref=
"urn%3Aurn-7%3A3gpp-service.ims.xxxx";
explicit;require
```

If there is an unauthenticated emergency session that is handed over from the packet switched do- main to the circuit switched domain, then the IMEI is the only identifier that is common to both do- mains [RFC 7255 [19]]

3. **UTRAN Cell ID**: The outgoing packets like `SIP REGISTER`, outgoing `SIP INVITE`, `SIP SUB- SCRIBE` messages contains the location information. This is sent in plain text, without encryption which is an important privacy concern.

For VoLTE:

```
P-Access-Network-Info:  3GPP-UTRAN-TDD;
utran-cell-id-3gpp=00000001
```

For VoWiFi:

```
P-Access-Network-Info:IEEE-802.11;
i-wlan-node-id=003a9axxxxxx
```

Such identifiers are also significant when it comes to spoofing attacks. The attack mentioned in A3 is an example.

4. **IMSI numbers:** The highlighted number is IMSI of O2 SIM that was used for making the call to our test phone [20]. This is found in SIP INVITE.

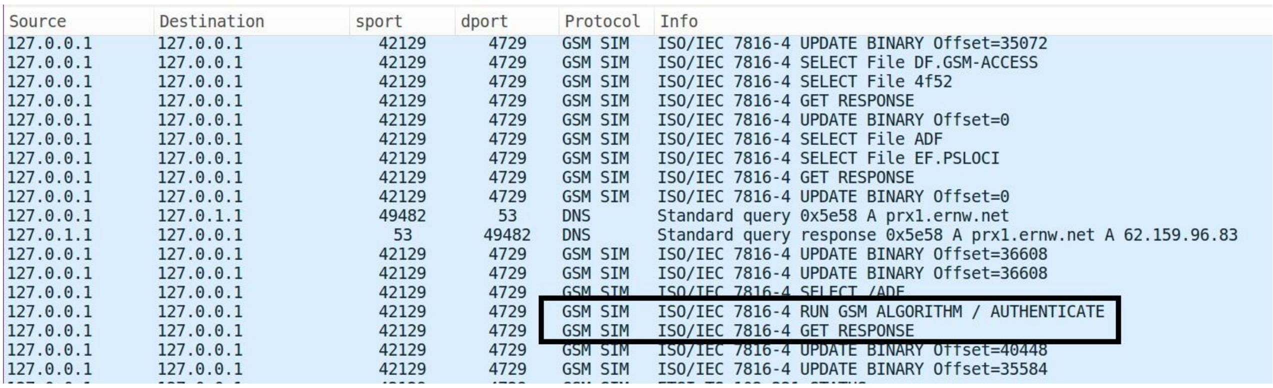
```
INVITE sip:262011202xxxx@[x.x.x.x]:6000
SIP/2.0
```

5. **Private IPs of server**: This is also found within SIP INVITE in incoming calls. These IPs are internal IPs of the provider or the phone.

```
To: <sip:+49151xxxxxxxx@62.xxx.xxx.xxx> From: <sip:+49176xxxxxxxx@10.xxx.xxx.xxx>;
tag=h7g4Esbg_mavodi-a-10b-3c-2-ffffffff-
_000050ED9CA4-1224-xxxx-xxxx
```

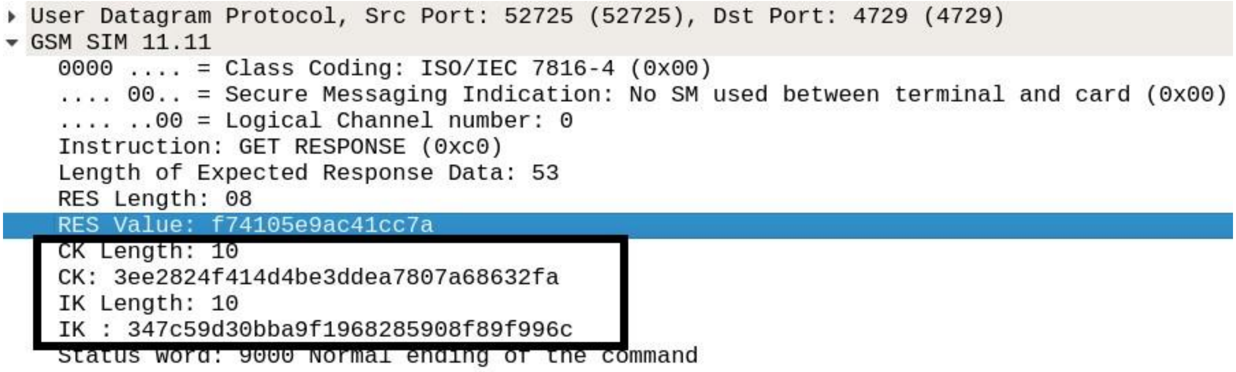
6.2 R2.1: Keys in GSM SIM

The `GSM SIM RESPONSE` can be parsed as shown in the Table 2. We wrote a Wireshark dissector that extract the keys from the GSM-SIM traffic as shown in Figure 11. The integrity key and the ciphering key can be seen in the packet dissection as shown in Figure 12.



```
Source      Destination    sport   dport  Protocol  Info
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 UPDATE BINARY Offset=35072
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 SELECT File DF.GSM-ACCESS
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 SELECT File 4f52
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 GET RESPONSE
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 UPDATE BINARY Offset=0
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 SELECT File ADF
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 SELECT File EF.PSLOCI
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 GET RESPONSE
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 UPDATE BINARY Offset=0
127.0.0.1   127.0.1.1      49482      53  DNS       Standard query 0x5e58 A prx1.ernw.net
127.0.1.1   127.0.0.1         53   49482  DNS       Standard query response 0x5e58 A prx1.ernw.net A 62.159.96.83
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 UPDATE BINARY Offset=36608
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 UPDATE BINARY Offset=36608
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 SELECT /ADF
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 RUN GSM ALGORITHM / AUTHENTICATE
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 GET RESPONSE
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 UPDATE BINARY Offset=40448
127.0.0.1   127.0.0.1      42129    4729  GSM SIM   ISO/IEC 7816-4 UPDATE BINARY Offset=35584
```

Figure 11: GSM SIM

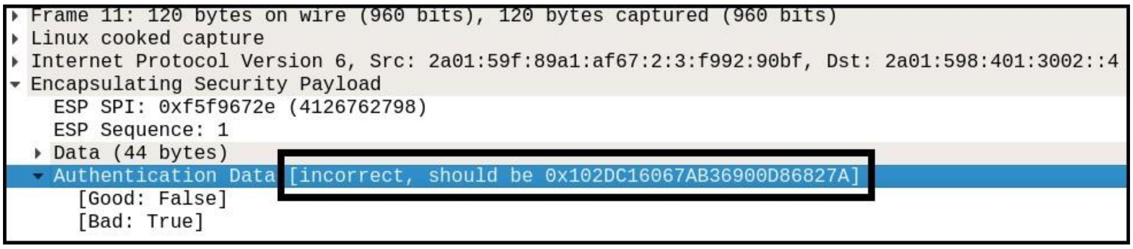


```
▸ User Datagram Protocol, Src Port: 52725 (52725), Dst Port: 4729 (4729)
▾ GSM SIM 11.11
    0000 .... = Class Coding: ISO/IEC 7816-4 (0x00)
    .... 00.. = Secure Messaging Indication: No SM used between terminal and card (0x00)
    .... ..00 = Logical Channel number: 0
    Instruction: GET RESPONSE (0xc0)
    Length of Expected Response Data: 53
    RES Length: 08
    RES Value: f74105e9ac41cc7a
    CK Length: 10
    CK: 3ee2824f414d4be3ddea7807a68632fa
    IK Length: 10
    IK : 347c59d30bba9f1968285908f89f996c
    Status Word: 9000 Normal ending of the command
```

Figure 12: Obtaining IK and CK from GSM-SIM

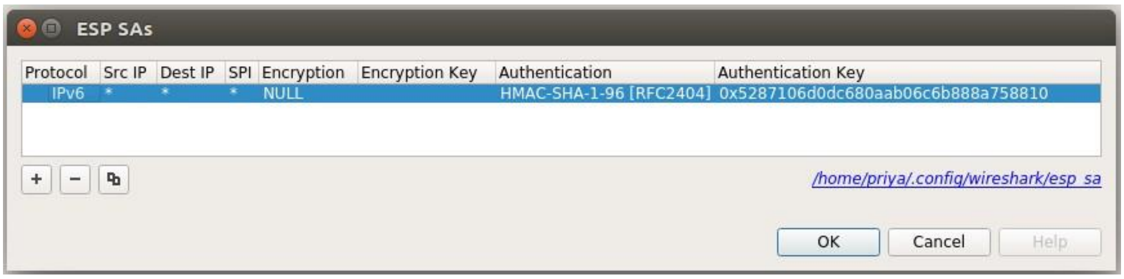
6.3 R2.2: Authentication using IK

We used Wireshark-Gcrypt library to validate if the keys we obtained is itself the key used for authentication. There is an option to set the Security Association (SA) in the packet preference of ESP. Without proper values for SA, the authentication fails as shown in Figure 13. The IPSec authentication algorithm is agreed during the SIP registration. Once we know the authentication algorithm (either from SIP register or by searching the logs) as well as integrity key that we obtained from the SIMTrace, we can establish the proper SA as a setting for Wireshark as shown in Figure 14. Providing the correct key (that we obtained by performing attack A2) will make the integrity check succeed as shown in Figure 15. This validates that the key extraction is correct and can be used for generating authentication value in ESP packets.



```
▸ Frame 11: 120 bytes on wire (960 bits), 120 bytes captured (960 bits)
▸ Linux cooked capture
▸ Internet Protocol Version 6, Src: 2a01:59f:89a1:af67:2:3:f992:90bf, Dst: 2a01:598:401:3002::4
▾ Encapsulating Security Payload
    ESP SPI: 0xf5f9672e (4126762798)
    ESP Sequence: 1
  ▸ Data (44 bytes)
  ▾ Authentication Data [incorrect, should be 0x102DC16067AB36900D86827A]
      [Good: False]
      [Bad: True]
```

Figure 13: Failed authentication check when keys don't match

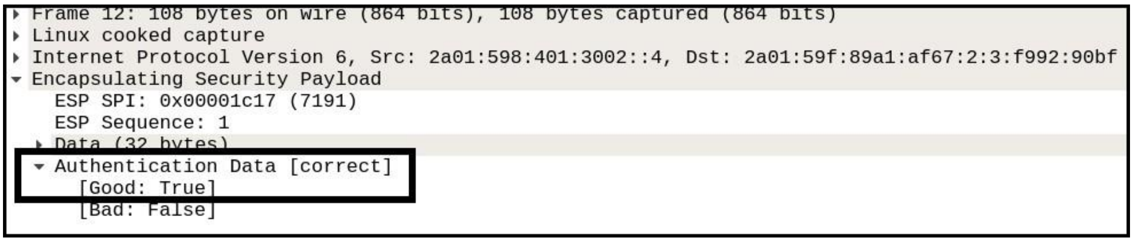


ESP SAs

Protocol	Src IP	Dest IP	SPI	Encryption	Encryption Key	Authentication	Authentication Key
IPv6	*	*	*	NULL		HMAC-SHA-1-96 [RFC2404]	0x5287106d0dc680aab06c6b888a758810

/home/priya/.config/wireshark/esp_sa

Figure 14: Establishing Security Association



```
▸ Frame 12: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
▸ Linux cooked capture
▸ Internet Protocol Version 6, Src: 2a01:598:401:3002::4, Dst: 2a01:59f:89a1:af67:2:3:f992:90bf
▾ Encapsulating Security Payload
    ESP SPI: 0x00001c17 (7191)
    ESP Sequence: 1
  ▸ Data (32 bytes)
  ▾ Authentication Data [correct]
      [Good: True]
      [Bad: False]
```

Figure 15: Successful authentication check when keys match

6.4 R3: User Location Manipulation

The attacker Evil sends an `SIP INVITE` request to Alice with a modified location. Evil uses SIP Proxy to send the crafted packet. The `P-Access-Network-ID` header value is modified to a fake value in the `SIP INVITE` from Evil sent to Alice. The header field is modified without an "np" (network-provided) attribute. It is observed that Alice receives the same SIP INVITE with the modified `P-Access-Network-ID` header value. Neither I-CSCF nor S-CSCF queried HSS to double check the user location.

6.5 R4: Roaming Information Manipulation

Evil sends a REGISTER request to IMS, which is exactly the same as a REGISTER request sent by normal user except that an extra header P-Visited-Network-ID is added with a value of “open-ims fake.test”. P- CSCF does not remove the inserted P-Visited-Network- ID header field. However, it just appends the network identity to the existing header field instead of adding an- other one. The request sent from P-CSCF to I-CSCF contains a P-Visited-Network-ID as shown below:

```
P-Visited-Network-ID:
open-ims_fake.test, open-ims.test
```

However, I-CSCF rejects the request. It replies with a SIP/2.0 403 Forbidden - HSS Roaming not allowed response because OpenIMS does not support roaming. But, in a real scenario, this attack might work based on the design choices made in I-CSCF and S-CSCF. It is ad- vised that P-CSCF should remove the header value if it is received directly from user and use it only if it is received from another network.

6.6 R5: Side channel

In our test, Evil sends an INVITE request to Alice containing a custom header field X-Header. This INVITE request is the same as an INVITE request from Evil to Alice, except for the additional custom header. X-Header will be populated with dummy data as shown in Figure 9. Two users can take advantage of this to exchange information without being charged. They can populate information in additional header fields to uncharged SIP requests such as OPTIONS request.

7 Mitigation

Compared to voice technologies over GSM and 3G, the voice calling over LTE and WiFi are more secure with additional security features in the architecture and with the help of IPSec. The IPSec (ESP) layer provides authentication and confidentiality (if encryption is enabled). This allows the user to be resistant to attacks such as IMSI catchers [21] or Silent message attacks[22] for location tracking. On the other hand, IPSec also provides protection to IMS against accounting bypass or spoofing attacks that targets the IMS rather than the UE.

However, this is made possible with the authentication of UE based on IPSec. The SIMTrace attack that sniffs at the ISIM interface for extracting the IPSec keys is one way to break the IPSec protection from the UE side. Even though it is hard to extract the shared secret from the ISIM, SIMTrace allows to extract the CK/IK that is generated from the shared secret. This gives power for an attacker to perform spoofing or other header manipulation attacks as mentioned in Section 4 (Attacks: A3, A4 and A5).

One mitigation against SIMTrace could be to use embedded SIM where the SIM card is fixed within the UE and cannot be separated allowing the SIMTrace to perform any sniffs. However, it is still possible for a skilled attacker to extract the SIM card out of an embedded SIM if he manages to not break the phone and handles necessary soldering. Security via obscurity cannot be considered an efficient solution. Thus, by design, a UE must always be considered as an untrusted device. This is an important design policy to keep in mind while building the IMS security policies.

- **Traffic monitoring**: To protect against SIP header fuzzing or header injection, there should be traffic monitoring in PDN gateways that performs deep packet inspection. There should be whitelist rules in place that determines the expected value in each header field.

- **Pre-defined ports**: In order to avoid malicious applications from using SIP signaling, there should be rules that allows only pre-defined ports.

- **Encryption**: `SIP REGISTER` message contained information such as IMSI and IMEI values in it. This is sent even before an IPSec session is established (in case of VoLTE). This can be exploited by a rogue IMS or a fake base station that acts as an IMSI catcher. There should be encryption in place before sending such information.

- **User awareness**: In [3] talks about WiFi based IMSI catcher that is applicable to VoWiFi. This attack is based on the fact that a rogue WiFi access point can simply perform the initial IKEv2 authentication where the UE tries to `REGISTER` by providing the IMSI value. In such scenarios, apart from a technical solution, user side mitigation and awareness can also help. Users must make sure not to connect their device to untrusted WiFis or provider connections by turning off data in case of suspicion.

8 Conclusion

In this paper, we demonstrated five attacks that looks at different layers of VoLTE/VoWiFi security. The first attack identifies important information disclosures such as IMEI, IMSI, location information and private IP of the server. In the second attack, A2, we identified a technique to extract the ciphering key and integrity key that are used for IPSec tunneling. Then we discuss three different kinds of injection attacks on the SIP header fields. We performed these attacks in an experimental setup using OpenIMS. However, we strongly believe that this can be reproduced in real network. When IPSec is in place, it is observed that injecting into the IPSec tunnel can be hard. However, we demonstrated that it is possible to obtain the IPSec keys from the phone easily. This can be used for generation of SIP packets with tampered SIP header fields from an attacker's perspective. This calls for the need of server side protection or mitigation against such attacks rather than relying on the IPSec tunnel and the obscurity in breaking the tunnel. Providers need to realize that IPSec is not the solution for SIP header injection attacks. As the attacker owns the UE, it is practically possible to easily obtain the IPSec keys even though the ISIM that generates the keys are protected within the USIM. To conclude, the key goal of this paper is to stress on the need of server side protection against injection attacks.

9 References

[1] Osmocom, "Simtrace." http://osmocom.org/projects/simtrace.

[2] Ericson, "World's first voice over lte services launched," 2012. Last Seen: May 2017.

[3] P. OHanlon and R. Borgaonkar, "WiFi-Based IMSI Catcher," 2016.

[4] P. O'Hanlon, R. Borgaonkar, and L. Hirschi, "Mobile subscriber wifi privacy," IEEE Symposium on Security and Privacy, 2017.

[5] C.-y. Li, G.-h. Tu, S. Lu, and X. Wang, "Insecurity of Voice Solution VoLTE in LTE Mobile Net- works," Proceedings of the 2015 ACM conference on Computer and communications security, 2015.

[6] G.-H. Tu, C.-Y. Li, C. Peng, and S. Lu, "How voice call technology poses security threats in 4g lte networks," in Communications and Network Security (CNS), 2015 IEEE Conference on, pp. 442–450, IEEE, 2015.

[7] H. Kim, D. Kim, M. Kwon, H. Han, Y. Jang, D. Han, T. Kim, and Y. Kim, "Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Misimplementations," Proceedings of the 2015 ACM conference on Computer and communications se- curity, 2015.

[8] F. Ozavci, VoIP Wars: The Phreakers Awaken. BlackHat USA, 2016.

[9] F. Ozavci, "Viproy 4.0." http://www.viproy.com/.

[10] A. Abolhadid, Exploitation of IMS in absence of confidentiality and integrity protection. 2017. https://insinuator.net/2017/02/exploitation-of-ims-in-absence- of-confidentiality-and-integrity-protection/.

[11] H. Schmidt and B. Butterly, IMSecure – Attacking VoLTE and more. 2016.

[12] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authen- tication and Key Agreement (EAP-AKA)." RFC 4187 (Informational), Jan. 2006. Updated by RFC 5448.

[13] 3GPP, "Characteristics of the ip multimedia services identity module (isim) application," TS 31.103, 3rd Generation Partnership Project (3GPP), 04 2011.

[14] M. Poikselka, H. Holma, J. Hongisto, J. Kallio, and A. Toskala, Voice over LTE (VoLTE). Wiley, 2014.

[15] "Openimscore." http://www.openimscore.org/.

[16] P. Haupt and M. Hurlimann, "Sip proxy voip security test tool," https://sourceforge.net/projects/sipproxy/.

[17] R. Jesske, K. Drage, and C. Holmberg, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP." RFC 7315 (Informational), July 2014.

[18] J. Peterson, C. Jennings, and R. Sparks, "Change Process for the Session Initiation Protocol (SIP) and the Real-time Applications and Infrastructure Area." RFC 5727 (Best Current Practice), Mar. 2010.

[19] A. Allen, " Using the International Mobile station Equipment Identity (IMEI) Uniform Resource Name (URN) as an Instance ID." RFC 7255 (Infor- mational), May 2014.

[20] "International mobile subscriber identity."

[21] D. Strobel, "Imsi catcher," in Chair for Communication Security, Ruhr Universitt Bochum, 2007.

[22] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," NDSS, 2016