Category Archives: 3G

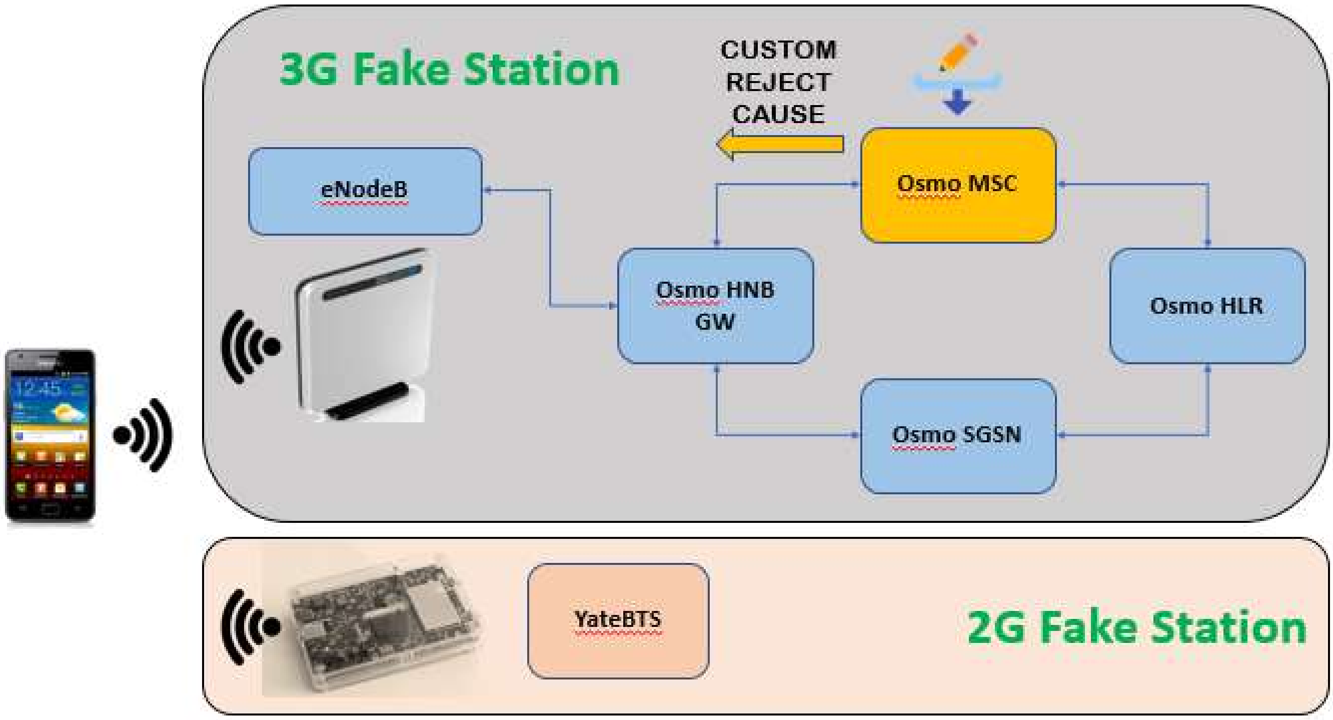
3G, CELLANALYSIS

IMSICATCHING ATTACKS ON 3G NETWORKS (PART 1)

OCTOBER 19, 2017 | 8 COMMENTS

In June of this year I announced the participation of CellAnalysis in the project of Sysmocom Accelerate 3g5 program to detect the 3G IMSICatching attacks. This article describes the first steps studying the 3G attacks within the Osmocom infrastructure and the basic principles of detection that are being implemented in CellAnalysis 3G.

Lab infrastructure:



Following the steps in the Getting_Started_with_3G tutorial, we setup the 3G network but we will modify the MSC node source code. We don't need to add any subscriber in the HLR/AuC database, since we are not going to deliver a 3G service to our victims. The negotiation procedure of the mobile to register in our 3G network will always be rejected, in order to be able to downgrade to 2G, in the same way as we saw in 4G (4G / LTE IMSI Catchers). In this first article we will use the “Location Update Reject” attack, with the different causes of rejection forcing the mobile to register in the 2G network (the downgrade attack).

Implementation:
3G

femtocell nano3G (Sysmocom)

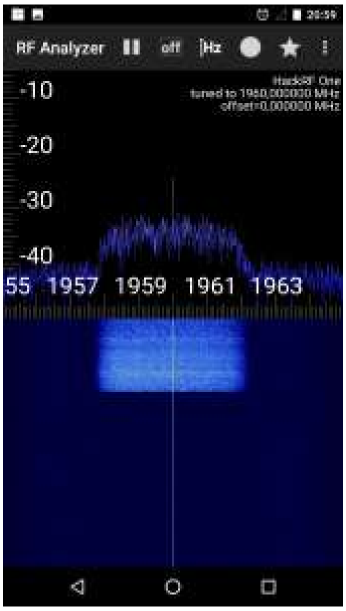
Osmocom 3G network, running on Ubuntu 14 (intel core i5 4200U 1,6GHz, 8Gb RAM)

2G

BladeRF x40

YateBTS, 2G network running on Ubuntu 16 (intel atom 1.6GHz, 8GB RAM)

Once configured the 3G network following the *Getting Started* tutorial, it’s better to verify that the cell 3G is transmitting correctly in the UARFCN 9800 (default channel):



HackRF One
tuned to 1960.000000 MHz
offset=0.000000 MHz

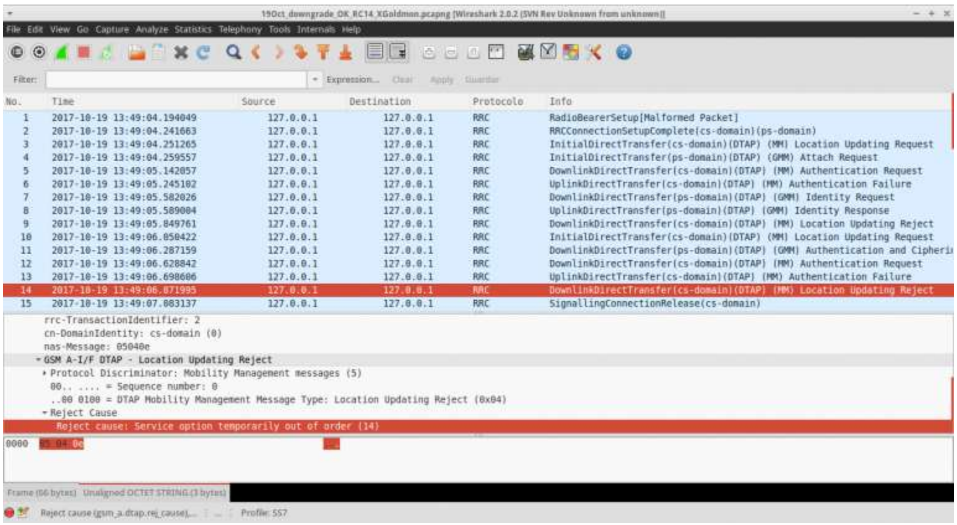
To implement our custom reject cause, we must modify the source code of the MSC to overwrite the registration reject cause in the “Location Update Request” response. Usually the reject cause should be “*(2) IMSI unknown in HLR*” since we have not provisioned any subscriber in our HLR or “*(3) Illegal MS*” if we only add the victim’s IMSI in the HLR Sqlite db but not the auth values. It’s needed to manipulate the source code of the MSC so that it always returns the cause value of our interest, according to whether we want to do a D.o.S or a 2G downgrade attack:

· Disable the USIM entirely until power-off or USIM removal.

· Attach requests disable the USIM for packets domain until power-off or USIM removal.

· Periodic Location Update requests will trigger the UE to attempt GERAN instead.

Once we choose and implement our attack, switch-on the victim mobile (S2) and activate Tobias Engel xgoldmon to detect the attack. Check the following image, how the response to the registration request (the Location Update Reject) is correctly sent to our victim with our reject cause choosen (this example is #14, "*Service option temporarily out of order*"):



19Oct_downgrade_OK_RC14_XGoldmon.pcapng [Wireshark 2.0.2 (SVN Rev Unknown from unknown)]

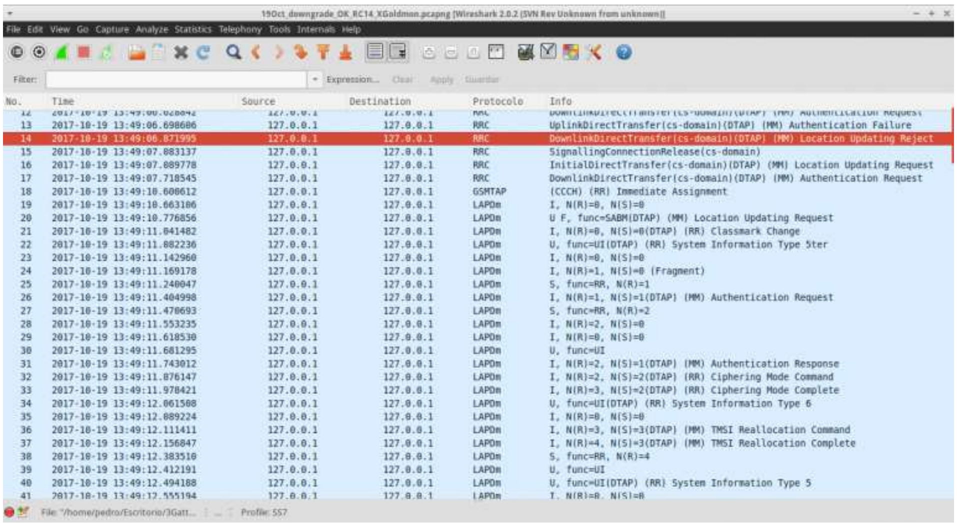
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Guardar

```
No.  Time                        Source      Destination  Protocolo  Info
 1   2017-10-19 13:49:04.194049  127.0.0.1   127.0.0.1    RRC        RadioBearerSetup[Malformed Packet]
 2   2017-10-19 13:49:04.241663  127.0.0.1   127.0.0.1    RRC        RRCConnectionSetupComplete(cs-domain)(ps-domain)
 3   2017-10-19 13:49:04.251265  127.0.0.1   127.0.0.1    RRC        InitialDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Request
 4   2017-10-19 13:49:04.259557  127.0.0.1   127.0.0.1    RRC        InitialDirectTransfer(ps-domain)(DTAP) (GMM) Attach Request
 5   2017-10-19 13:49:05.142057  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Authentication Request
 6   2017-10-19 13:49:05.245102  127.0.0.1   127.0.0.1    RRC        UplinkDirectTransfer(cs-domain)(DTAP) (MM) Authentication Failure
 7   2017-10-19 13:49:05.582026  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(ps-domain)(DTAP) (GMM) Identity Request
 8   2017-10-19 13:49:05.589004  127.0.0.1   127.0.0.1    RRC        UplinkDirectTransfer(ps-domain)(DTAP) (GMM) Identity Response
 9   2017-10-19 13:49:05.849761  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Reject
10   2017-10-19 13:49:06.050422  127.0.0.1   127.0.0.1    RRC        InitialDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Request
11   2017-10-19 13:49:06.287159  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(ps-domain)(DTAP) (GMM) Authentication and Cipheri
12   2017-10-19 13:49:06.628842  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Authentication Request
13   2017-10-19 13:49:06.698606  127.0.0.1   127.0.0.1    RRC        UplinkDirectTransfer(cs-domain)(DTAP) (MM) Authentication Failure
14   2017-10-19 13:49:06.871995  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Reject
15   2017-10-19 13:49:07.883137  127.0.0.1   127.0.0.1    RRC        SignallingConnectionRelease(cs-domain)
```

```
      rrc-TransactionIdentifier: 2
      cn-DomainIdentity: cs-domain (0)
      nas-Message: 05040e
    ▾ GSM A-I/F DTAP - Location Updating Reject
     ▸ Protocol Discriminator: Mobility Management messages (5)
       00.. .... = Sequence number: 0
       ..00 0100 = DTAP Mobility Management Message Type: Location Updating Reject (0x04)
     ▾ Reject Cause
         Reject cause: Service option temporarily out of order (14)
0000  05 04 0e
```

Frame (56 bytes) Unaligned OCTET STRING (3 bytes)
Reject cause (gsm_a.dtap.rej_cause)...
Profile: SS7

After the LocUp Reject, the victim mobile connects to the 2G network (YateBTS). See bellow how after the RRC message "*Location Update Reject*", the mobile starts to use LAPDm and begins the authentication in the 2G network:

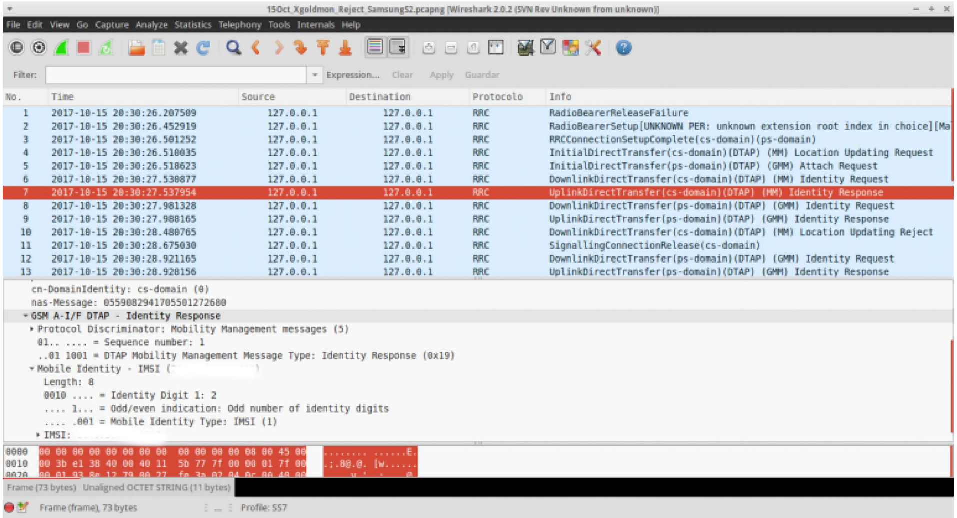


19Oct_downgrade_OK_RC14_XGoldmon.pcapng [Wireshark 2.0.2 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Guardar

```
No.  Time                        Source      Destination  Protocolo  Info
12   2017-10-19 13:49:06.628842  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Authentication Request
13   2017-10-19 13:49:06.698606  127.0.0.1   127.0.0.1    RRC        UplinkDirectTransfer(cs-domain)(DTAP) (MM) Authentication Failure
14   2017-10-19 13:49:06.871995  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Reject
15   2017-10-19 13:49:07.883137  127.0.0.1   127.0.0.1    RRC        SignallingConnectionRelease(cs-domain)
16   2017-10-19 13:49:07.889778  127.0.0.1   127.0.0.1    RRC        InitialDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Request
17   2017-10-19 13:49:07.718545  127.0.0.1   127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Authentication Request
18   2017-10-19 13:49:10.600612  127.0.0.1   127.0.0.1    GSMTAP     (CCCH) (RR) Immediate Assignment
19   2017-10-19 13:49:10.663106  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=0, N(S)=0
20   2017-10-19 13:49:10.776856  127.0.0.1   127.0.0.1    LAPDm      U F, func=SABM(DTAP) (MM) Location Updating Request
21   2017-10-19 13:49:11.041482  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=0, N(S)=0(DTAP) (RR) Classmark Change
22   2017-10-19 13:49:11.082236  127.0.0.1   127.0.0.1    LAPDm      U, func=UI(DTAP) (RR) System Information Type 5ter
23   2017-10-19 13:49:11.142960  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=0, N(S)=0
24   2017-10-19 13:49:11.169178  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=1, N(S)=0 (Fragment)
25   2017-10-19 13:49:11.240047  127.0.0.1   127.0.0.1    LAPDm      S, func=RR, N(R)=1
26   2017-10-19 13:49:11.404998  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=1, N(S)=1(DTAP) (MM) Authentication Request
27   2017-10-19 13:49:11.470693  127.0.0.1   127.0.0.1    LAPDm      S, func=RR, N(R)=2
28   2017-10-19 13:49:11.553235  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=2, N(S)=0
29   2017-10-19 13:49:11.618530  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=0, N(S)=0
30   2017-10-19 13:49:11.681295  127.0.0.1   127.0.0.1    LAPDm      U, func=UI
31   2017-10-19 13:49:11.743012  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=2, N(S)=1(DTAP) (MM) Authentication Response
32   2017-10-19 13:49:11.876147  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=2, N(S)=2(DTAP) (RR) Ciphering Mode Command
33   2017-10-19 13:49:11.978421  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=3, N(S)=2(DTAP) (RR) Ciphering Mode Complete
34   2017-10-19 13:49:12.061508  127.0.0.1   127.0.0.1    LAPDm      U, func=UI(DTAP) (RR) System Information Type 6
35   2017-10-19 13:49:12.089224  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=0, N(S)=0
36   2017-10-19 13:49:12.111411  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=3, N(S)=3(DTAP) (MM) TMSI Reallocation Command
37   2017-10-19 13:49:12.156847  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=4, N(S)=3(DTAP) (MM) TMSI Reallocation Complete
38   2017-10-19 13:49:12.383510  127.0.0.1   127.0.0.1    LAPDm      S, func=RR, N(R)=4
39   2017-10-19 13:49:12.412191  127.0.0.1   127.0.0.1    LAPDm      U, func=UI
40   2017-10-19 13:49:12.494188  127.0.0.1   127.0.0.1    LAPDm      U, func=UI(DTAP) (RR) System Information Type 5
41   2017-10-19 13:49:12.555194  127.0.0.1   127.0.0.1    LAPDm      I, N(R)=0, N(S)=0
```

But, before switching to 2G network, the registration procedure has asked the victim mobile to identify, by requesting the IMSI. This is the 3G IMSICatching attack, see the "*Identity Response*" message (IMSI has been removed in the image):


15Oct_Xgoldmon_Reject_SamsungS2.pcapng [Wireshark 2.0.2 (SVN Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression...
Clear
Apply
Guardar

```
No.  Time                        Source       Destination  Protocolo  Info
1    2017-10-15 20:30:26.207509  127.0.0.1    127.0.0.1    RRC        RadioBearerReleaseFailure
2    2017-10-15 20:30:26.452919  127.0.0.1    127.0.0.1    RRC        RadioBearerSetup[UNKNOWN PER: unknown extension root index in choice][Ma
3    2017-10-15 20:30:26.501252  127.0.0.1    127.0.0.1    RRC        RRCConnectionSetupComplete(cs-domain)(ps-domain)
4    2017-10-15 20:30:26.510035  127.0.0.1    127.0.0.1    RRC        InitialDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Request
5    2017-10-15 20:30:26.518623  127.0.0.1    127.0.0.1    RRC        InitialDirectTransfer(ps-domain)(DTAP) (GMM) Attach Request
6    2017-10-15 20:30:27.530877  127.0.0.1    127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Identity Request
7    2017-10-15 20:30:27.537954  127.0.0.1    127.0.0.1    RRC        UplinkDirectTransfer(cs-domain)(DTAP) (MM) Identity Response
8    2017-10-15 20:30:27.981328  127.0.0.1    127.0.0.1    RRC        DownlinkDirectTransfer(ps-domain)(DTAP) (GMM) Identity Request
9    2017-10-15 20:30:27.988165  127.0.0.1    127.0.0.1    RRC        UplinkDirectTransfer(ps-domain)(DTAP) (GMM) Identity Response
10   2017-10-15 20:30:28.480765  127.0.0.1    127.0.0.1    RRC        DownlinkDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Reject
11   2017-10-15 20:30:28.675030  127.0.0.1    127.0.0.1    RRC        SignallingConnectionRelease(cs-domain)
12   2017-10-15 20:30:28.921165  127.0.0.1    127.0.0.1    RRC        DownlinkDirectTransfer(ps-domain)(DTAP) (GMM) Identity Request
13   2017-10-15 20:30:28.928156  127.0.0.1    127.0.0.1    RRC        UplinkDirectTransfer(ps-domain)(DTAP) (GMM) Identity Response
```

```
    cn-DomainIdentity: cs-domain (0)
    nas-Message: 0559082941705501272680
  ▾ GSM A-I/F DTAP - Identity Response
    ▸ Protocol Discriminator: Mobility Management messages (5)
      01.. .... = Sequence number: 1
      ..01 1001 = DTAP Mobility Management Message Type: Identity Response (0x19)
    ▾ Mobile Identity - IMSI ([redacted])
        Length: 8
        0010 .... = Identity Digit 1: 2
        .... 1... = Odd/even indication: Odd number of identity digits
        .... .001 = Mobile Identity Type: IMSI (1)
      ▸ IMSI: [redacted]
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ........ ......E.
0010  00 3b e1 38 40 00 40 11  5b 77 7f 00 00 01 7f 00   .;.8@.@. [w......
0020  00 01 93 8c 12 79 00 27  fe 3a 02 04 0c 00 40 00
```

Frame (73 bytes) Unaligned OCTET STRING (11 bytes) [redacted]

Frame (frame), 73 bytes   Profile: SS7

Detection:

CellAnalysis 3G uses active monitoring solutions (in this article xgoldmon), instead of the passive ones as SDR boards used in the 2G fake stations detection, to monitor 3G attacks.

Advantages using active monitoring;

- ciphering algorithms (UEA) usage
- authentication parameters and rates

But on the other hand, there is a big disadvantage:

- one SIM card and device per operator in order to scan all the 3G fake stations

Of course a regulation compliance check is being carried out to determine wether the 3G radio parameters are used accordingly to each country frequency distribution regulation, as in the 2G detection.

3G, CELLANALYSIS

CELLANALYSIS 3G AND OSMOCOM 3.5G

MAY 30, 2017 | LEAVE A COMMENT

For a few years now I've focused on improving the unpublished version of CellAnalysis (currently 0.1.10), using it in security audits and trying to know the best way to protect the algorithms of the code in order to publish in the future the full version.

I recently decided to give a new direction to CellAnalysis to be able also to detect the fake 3G cells used to force the victims to use fake 2G stations (downgrade attacks). As initial tool I'm thinking in Xgoldmon, which will allow us to analyze the signaling of a mobile in an active way (we need a SIM card inside), although the goal that I have marked in the long term is to write a GNURadio tool that will allow to monitor broadcast traffic in 3G passively, without the need of a SIM card , using the standard SDR (BladeRF) boards.

On the other hand, I had the great luck to participate in the project to contribute to Osmocom 3G5 to cover the following objectives:

(**Short term**) Study how to implement in the Osmocom 3G network the following attacks:

3G IMSI Catching attacks, using RRC Connection Request/Reject (Initial UE identity – IMSI)

2G downgrade attacks, based on "Loc.Up.Req" reject codes and "RRC Connection Reject"

(**Short term**) Use Xgoldmon software adapting CellAnalysis algorithms in order to detect the two previous attacks.

(**Long term**) Write GNURadio scripts/blocks to decode 3G broadcast traffic, adapting CellAnalysis to detect previous attacks with SDR boards.

I would like to give **special thanks** to **@sysmocom**, **Osmocom community** and the "Accelerate 3g5 program" for their contributions to this project.