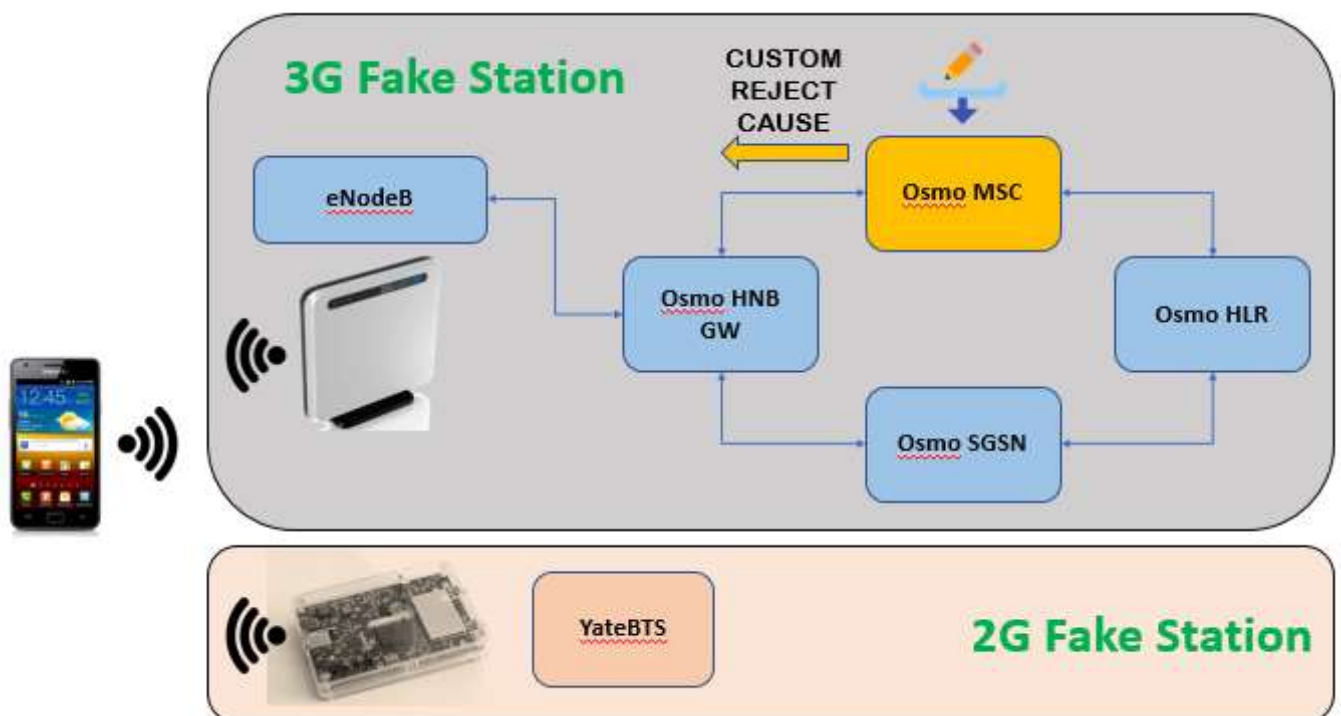


IMSI CATCHING ATTACKS ON 3G NETWORKS (PART 1)

OCTOBER 19, 2017 | PEDRO | 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 IMSI Catching 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)

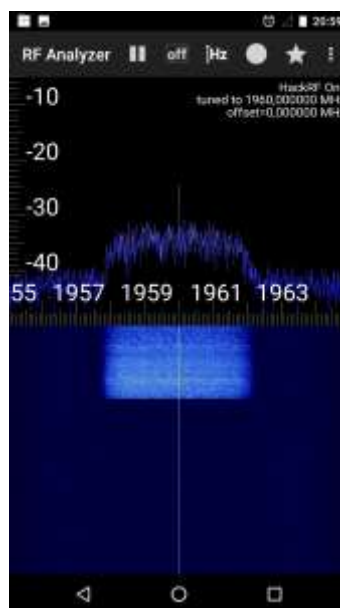
Osmocom 3G network, running on Ubuntu 14 (intel core i5 4200U 1,6GHz, 8Gb RAM)

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):



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 chosen (this example is #14, “Service option temporarily out of order”):

No.	Time	Source	Destination	Protocol	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(cs-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 13:49:05.245182	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 13:49:06.058422	127.0.0.1	127.0.0.1	RRC	InitialDirectTransfer(cs-domain)(DTAP) (MM) Location Updating Request
11	2017-10-19 13:49:06.207159	127.0.0.1	127.0.0.1	RRC	DownlinkDirectTransfer(ps-domain)(DTAP) (GMM) Authentication and Ciphering Mode Command
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 13:49:07.083137	127.0.0.1	127.0.0.1	RRC	SignallingConnectionRelease(cs-domain)

Packet 14 details:

```

rrc-TransactionIdentifier: 2
cs-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
  
```

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

No.	Time	Source	Destination	Protocol	Info
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 13:49:07.083137	127.0.0.1	127.0.0.1	RRC	SignallingConnectionRelease(cs-domain)
16	2017-10-19 13:49:07.089778	127.0.0.1	127.0.0.1	RRC	InitialDirectTransfer(cs-domain)(DTAP) (MM) Authentication 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 13:49:10.606612	127.0.0.1	127.0.0.1	GSM-TAP	(CCCH) (RR) Immediate Assignment
19	2017-10-19 13:49:10.663186	127.0.0.1	127.0.0.1	LAPDm	I, N(R)=0, N(S)=0
20	2017-10-19 13:49:10.776056	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 13:49:11.062236	127.0.0.1	127.0.0.1	LAPDm	U, func=UI(DTAP) (RR) System Information Type 5
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 13:49:12.061500	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 13:49:12.412181	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):

Sorry for the delay. I didn't use OpenBTS-UMTS, but I guess should be feasible as you can modify the source code to adapt the reject procedure, in order to deny access with custom reject cause.

Regards,
Pedro



d4st

APRIL 10, 2018 AT 6:18 PM

is it possible to see your modification about MSC code!? any diff or like that for having inspiration !? and the what is the periodicity of the location update !?



★ **pedro**

APRIL 10, 2018 AT 7:40 PM

Hi d4st,

Inspiration could be found by using "grep" command, so you should locate in the source code the specific files managing the reject causes (very easy).

About your second question, I suggest you start reading the document "3GPP TS 23.012" -> "Detailed procedure in the MSC" and "3GPP TR 29.994" could be interesting for you, among others.

Regards,
Pedro



d4st

APRIL 11, 2018 AT 3:41 AM

hi pedro, is it possible to configure any periodic location update by configuring the T3212 or it's only for the GSM-GPRS configuration?



★ **pedro**

APRIL 11, 2018 AT 8:16 PM

Hi d4st,

Yes, there is a periodic location update timer in both 2G (osmo-bsc) and 3G (osmo-msc):

osmobsc-vty-reference.pdf: "1.15.45 periodic location update <6-1530>"

osmomsc-vty-reference.pdf: "1.14.9 periodic location update <6-1530>"

Regards,
Pedro



d4st

APRIL 12, 2018 AT 3:45 AM

Thank you very much! hopping the part2 is coming soon ! is it possible to have any video about your conferences about 'CellAnalysis at DefCon DemoLabs' when i try to google it i can't find any links. Great tutorial, and thanks for all explanation



d4st

APRIL 12, 2018 AT 2:51 PM

And it's not possible to integrate any redirect carrier info with this lu-reject !? what standartisation specifie this on 3GPP on TSXX.XX!?