OsmoSGSN - Bug #2958

OsmoSGSN doesn't authenticate on second/further ATTACH REQUEST

02/17/2018 05:29 PM - laforge

Status:	Stalled	**Start date:**	02/17/2018
Priority:	Normal	**Due date:**	
Assignee:	sysmocom	**% Done:**	50%
Category:			
Target version:			
Spec Reference:			

Description

When a new/unknown MS performs an ATTACH REQUEST for the first time, it is authenticated.

However, if that same MS later performs a second ATTACH REQUEST, even with new P-TMSI/TLLI, it is not authenticated and we simply send an ATTACH ACCEPT. This is a security problem, as it means anyone can impersonate other known-existing IMSIs.

Related issues:

Related to OsmoSGSN - Bug #3302: implement a FSM for GMM Attach Request	**Closed**	**05/29/2018**

History

#1 - 04/10/2018 05:34 PM - laforge

- Assignee changed from sysmocom to lynxis

#2 - 05/02/2018 06:16 PM - lynxis

- Status changed from New to In Progress

#3 - 05/29/2018 04:40 PM - lynxis

- Status changed from In Progress to Stalled

- % Done changed from 0 to 50

I've started to refactor the whole GMM Attach Request handling into one fsm.
This issue is already fixed in the new fsm implementation.
I've created the ttcn3 testcase

```
SGSN_Tests.TC_attach_second_attempt
```

for this.

#4 - 05/29/2018 04:40 PM - lynxis

- Related to Bug #3302: implement a FSM for GMM Attach Request added

#5 - 05/30/2018 02:18 PM - laforge

- Tags set to TTCN3

#6 - 06/12/2018 01:18 PM - lynxis

#7 - 08/07/2018 06:28 PM - lynxis

~~The test is failing again, even under the new FSM.~~
~~The HLR integration into the test must be rewritten.~~

At the moment, the TTCN test case **SGSN_Tests.TC_attach_second_attempt** still fails, but this is fails, because the second attach does not proceed, because TTCN explicit expect to see an **Insert Subscriber Data Request**.
This request will be never sent from the SGSN, because it has still valid key data.

#8 - 04/15/2019 07:37 AM - laforge

#9 - 04/18/2019 11:20 AM - lynxis

- Status changed from Stalled to In Progress

#10 - 04/18/2019 03:30 PM - lynxis

- Priority changed from High to Normal

It's not only the SGSN Tests. The SGSN does not behave correctly. The sgsn_authentication have to be rewritten as well the integration of Auth Req/Response to fix the real problem.

#11 - 07/18/2019 05:11 AM - laforge

- Status changed from In Progress to Stalled

#12 - 01/08/2020 10:49 PM - laforge

- Assignee changed from lynxis to sysmocom

Files

20180216-sgsn-second-attach-no-auth.pcap	2.37 KB	02/17/2018	laforge