OsmoSGSN - Support #3920

PCAPs files of 3G PS for Osmocom network and Commercial one

04/12/2019 12:51 PM - efistokl

Status:	In Progress	**Start date:**	04/12/2019
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Iu interface		
Target version:			
Spec Reference:			

Description

In iphone-6s-q.pcap - commercial software, trace taken on 10.0.2.195:
(around between 10:22:44 and 10:23:17 I didn't have internet, maybe temporary fail of the system to respond to the packet 10754. All other time the data was working)
10.0.2.199 - nano3g ip.access S8
10.0.2.195 - (not osmocom) core network (without HLR and GGSN)
10.0.1.123 or 192.168.14.16 (same host) - GGSN and HLR

In iphone-6s-osmocom.pcap - osmocom based system. Data stopped working around 10:05:59 (time in the trace, or packet 3727), trace taken on 10.0.2.51:
10.0.2.52 - nano3g ip.access S8
10.0.2.51 - osmocom host (without HLR and GGSN)
10.0.1.123 or 192.168.14.16 (same host) - GGSN
172.48.1.5 - HLR

At first glance it seems that Osmo-SGSN doesn't respond properly to (GMM) Service Requests which come some time after initial PS activation. I haven't inspected the traces thoroughly yet.

Related issues:

Related to OsmoSGSN - Bug #1977: 3G IuPS is unreliable	**Closed**	**03/09/2017**
Related to OsmoSGSN - Bug #3936: Iu: first GMM Service Request does not find ...	**New**	**04/16/2019**
Related to OsmoSGSN - Bug #3923: Iu: Respond to SecurityCommandReject messages	**New**	**04/14/2019**
Related to OsmoSGSN - Bug #3937: Iu: verify handling of GMM Service Request (...	**In Progress**	**04/16/2019**
Related to OsmoSGSN - Bug #3922: Iu: send RANAP CommonID to known connection	**Closed**	**04/13/2019**

History

#1 - 04/13/2019 11:09 AM - laforge

It looks also like there might be some problem with setting up air interface security? The last commands we're seeing is the SecurityModeCommand from SGSN to hNodeB, and then there's long silence. 30s later the Iu connection is released. However, the "outcome" is successful?

One difference is that the KeyStatus is "old" in OsmoSGSN case, but "new" in the proprietary SGSN case. However, that is probably explained by the fact that in the proprietary case, GMM authentication happens between the service request and the SecurityModeCommand, while OsmoSGSN doesn't re-authenticate on every service request. AFAIK both are valid scenarios.

Another difference is that the proprietary SGSN is explicitly sending "EncryptionInformation = no-encryption" in he SecurityModeCommand (which the hNodeB also confirms), whereas the OsmoSGSN simply doesn't sent the entire EncryptionInformation protocolIE. OsmoSGSN only includes the protocolIE for IntegrityProtection, but not Encryption.

After the successful SecurityModeComplete with the proprietary SGSN, the hNodeB is sending a RAB-AssignmentRequest. This is never received from the hNodeB in the non-working case with OsmoSGSN. Hence my suspicion that something is going wrong when setting up air interface security.

#2 - 04/13/2019 11:26 AM - laforge

- Related to Bug #1977: 3G IuPS is unreliable added

#3 - 04/14/2019 12:24 AM - lynxis

The MS tries to get a RAB assignment via the Service Request, but never got an answer. In theory we could send it already together with the PDP Context Activate.

The SGSN have to answer the Service Request.

#4 - 04/14/2019 11:34 AM - laforge

lynxis wrote:

> The MS tries to get a RAB assignment via the Service Request, but never got an answer. In theory we could send it already together with the PDP Context Activate.
> The SGSN have to answer the Service Request.

This is not matching my understanding. The CM SERVICE REQUEST doesn't trigger the RAB Assignment in the SGSN. The MS/UE should send a RAB-AssignmentRequest to us, and that's what triggers the RAB-Assignment.

As the MS is never sending the RAB-AssignmentRequeest (or at leaset the SGSN doesnt' receive it), I suspect something goes wrong before (SecurityModeControl, ...)

#5 - 04/14/2019 08:29 PM - lynxis

23.060 6.12.1 describes it. A Service Request (type=DATA) should trigger the RAB AssignmentRequest. The RAB AssignmentRequest is sent by the SGSN to the RNC/UE.
After an IU release, the RAB Assignment must be sent again and this is done via a Service Request.

The sgsn in gprs_gmm.c:1088 should sent it out.

Because there is a SecurityMode Complete, I would expect it succeed also on the MS side.
Why is the SGSN not sending out the RAB Assignments?

efistokl can you do another run with SGSN logging to debug and attach it here?

#6 - 04/14/2019 09:22 PM - efistokl

lynxis wrote:

> 23.060 6.12.1 describes it. A Service Request (type=DATA) should trigger the RAB AssignmentRequest. The RAB AssignmentRequest is sent by the SGSN to the RNC/UE.
> After an IU release, the RAB Assignment must be sent again and this is done via a Service Request.
>
> The sgsn in gprs_gmm.c:1088 should sent it out.
>
> Because there is a SecurityMode Complete, I would expect it succeed also on the MS side.
> Why is the SGSN not sending out the RAB Assignments?
>
> efistokl can you do another run with SGSN logging to debug and attach it here?

yes, I will do that. I will try to do that today (Monday) with the setup I have here (I am at a different place now). Otherwise, I will do that on Tuesday upon my return.

#7 - 04/14/2019 10:13 PM - laforge

On Sun, Apr 14, 2019 at 08:29:47PM +0000, lynxis [REDMINE] wrote:

> 23.060 6.12.1 describes it. A Service Request (type=DATA) should trigger the RAB AssignmentRequest. The RAB AssignmentRequest is sent by the SGSN to the RNC/UE.
> After an IU release, the RAB Assignment must be sent again and this is done via a Service Request.

Thanks for correcting me. Seems like I was confused after not working with IuPS for quite some time.

#8 - 04/15/2019 01:18 PM - efistokl

- File sgsn-10.0.3.19.logs.txt added

- File iphone-6s-osmocom-10.0.3.19.pcap added

lynxis wrote:

> 23.060 6.12.1 describes it. A Service Request (type=DATA) should trigger the RAB AssignmentRequest. The RAB AssignmentRequest is sent by the SGSN to the RNC/UE.

> After an IU release, the RAB Assignment must be sent again and this is done via a Service Request.
>
> The sgsn in gprs_gmm.c:1088 should sent it out.
>
> Because there is a SecurityMode Complete, I would expect it succeed also on the MS side.
> Why is the SGSN not sending out the RAB Assignments?
>
> @ efistokl can you do another run with SGSN logging to debug and attach it here?

lynxis sorry for me being slow to respond, I am travelling right now.
Trace and SGSN logs attached.
Note: for some reason it appears that there are no GSUP messages in the trace. All other behavior seems to be identical to the systems I used for other traces attached to this issue. (I had to use another setup as I am in a different location at the moment).

If the trace or logs are not good enough, I can retake them (I can do that on 10.0.2.51 system upon my return as I did before)

In iphone-6s-osmocom-10.0.3.19.pcap - Data stopped working around after Iu-ReleaseRequest (as expected) (packet 3623), trace taken on 10.0.3.19:
10.0.3.20 - nano3g ip.access S8, same firmware as on other S8 I used before
10.0.3.19 - osmocom host (without HLR and GGSN)
10.0.1.123 or 192.168.14.16 (same host) - GGSN
172.48.1.5 - HLR

#9 - 04/15/2019 01:36 PM - lynxis

efistokl Don't get you stressed :). Your log helped a lot! I've found a bug.

Sadly to say. It was me, who broke it, when introducing the GMM Attach FSM.

#10 - 04/15/2019 01:45 PM - lynxis

The log shows:

```
Apr 15 15:53:00 Osmocom osmo-sgsn[3090]: <0002> gprs_gmm.c:1860 MM(---/ffffffff) -> GMM SERVICE REQUEST MI(362
9027335) type="data"
Apr 15 15:53:00 Osmocom osmo-sgsn[3090]: <0018> gprs_gmm.c:205 Cannot find mm ctx for IU event 1
```

It should know the mm ctx! Why can't it find a MM ctx for the request?

The problem here is the SGSN doesn't do anything with Security Command Complete anymore, except for GMM Attach procedures, but it can **find** an MM CTX

```
Apr 15 15:53:34 Osmocom osmo-sgsn[3090]: <0002> gprs_gmm.c:1860 MM(---/ffffffff) -> GMM SERVICE REQUEST MI(362
9027335) type="data"
Apr 15 15:53:34 Osmocom osmo-sgsn[3090]: <0002> gprs_gmm.c:208 GMM_ATTACH_REQ_FSM(gb_gmm_req)[0x15b9b70]{Init}
: Received Event IU Security Command Complete received.
Apr 15 15:53:34 Osmocom osmo-sgsn[3090]: <0002> gprs_gmm.c:208 GMM_ATTACH_REQ_FSM(gb_gmm_req)[0x15b9b70]{Init}
: Event IU Security Command Complete received. not permitted
```

#11 - 04/16/2019 07:10 AM - lynxis

- Status changed from New to In Progress

efistokl can you please test https://gerrit.osmocom.org/#/c/osmo-sgsn/+/13654/

#12 - 04/16/2019 05:47 PM - efistokl

- File after-patch-gerrit-13654.zip added

lynxis wrote:

> @ efistokl can you please test https://gerrit.osmocom.org/#/c/osmo-sgsn/+/13654/

lynxis logs and traces are in zip.

I've performed tests with both iphone 6s and huawei ale l 21 phones (same SIM).

Huawei seems to be fine. I see both "(GMM) Service Accept" messages and "RAB-AssignmentRequest" messages

For Iphone I still see

```
... iu_client.c:599 Error in cn_ranap_handle_co (-1)
```

the system sends only "(GMM) Service Accept", no "RAB-AssignmentRequest".

System description:
trace taken on 10.0.2.51:
10.0.2.52 - nano3g ip.access S8
10.0.2.51 - osmocom host (without HLR and GGSN)
10.0.1.123 or 192.168.14.16 (same host) - GGSN
172.48.1.5 - HLR

#13 - 04/16/2019 06:12 PM - efistokl

efistokl wrote:

> I've performed tests with both iphone 6s and huawei ale l 21 phones (same SIM).
> Huawei seems to be fine. I see both "(GMM) Service Accept" messages and "RAB-AssignmentRequest" messages
> For Iphone I still see
> [...]
> the system sends only "(GMM) Service Accept", no "RAB-AssignmentRequest".

I will recheck tomorrow again. The system here behaves a bit weird now.

#14 - 04/16/2019 06:22 PM - lynxis

- Related to Bug #3936: Iu: first GMM Service Request does not find a MM ctx added

#15 - 04/16/2019 06:41 PM - lynxis

efistokl maybe the iphone expect an iu release after the pdp context accept. The missing rab assignment on it's Service Request could be a problem of the second PDP Request/Reject. I don't know if the SGSN is handling this correctly. I've to read the code to confirm or reject the thesis.

#16 - 04/16/2019 06:56 PM - lynxis

- Related to Bug #3923: Iu: Respond to SecurityCommandReject messages added

#17 - 04/16/2019 06:57 PM - lynxis

- Related to Bug #3937: Iu: verify handling of GMM Service Request (data)when no PDP Context present. added

#18 - 04/16/2019 06:59 PM - lynxis

- Related to Bug #3922: Iu: send RANAP CommonID to known connection added

#19 - 04/18/2019 11:45 AM - efistokl

- File experiment-thu-18-4-19.zip added

Some experimenting: Commented out the body of "mmctx_change_gtpu_endpoints_to_sgsn" which did get called when the UE sent Iu-ReleaseRequest (presumably due to user inactivity). So that Update PDP Context Request wasn't sent to GGSN and the PDP context didn't get deleted a moment later (due to sending "Error Indication"). Traces and logs attached (System same as before).

```
--- a/src/gprs/gprs_gmm.c
+++ b/src/gprs/gprs_gmm.c
@@ -117,14 +117,14 @@ static int gsm48_gmm_authorize(struct sgsn_mm_ctx *ctx);

 static void mmctx_change_gtpu_endpoints_to_sgsn(struct sgsn_mm_ctx *mm_ctx)
 {
-       struct sgsn_pdp_ctx *pdp;
-       llist_for_each_entry(pdp, &mm_ctx->pdp_list, list) {
-               LOGMMCTXP(LOGL_INFO, mm_ctx, "Changing GTP-U endpoints %s -> %s\n",
-                         sgsn_gtp_ntoa(&pdp->lib->gsnlu), inet_ntoa(sgsn->cfg.gtp_listenaddr.sin_addr));
-               sgsn_pdp_upd_gtp_u(pdp,
-                                  &sgsn->cfg.gtp_listenaddr.sin_addr,
-                                  sizeof(sgsn->cfg.gtp_listenaddr.sin_addr));
```

```
-       }
+       // struct sgsn_pdp_ctx *pdp;
+       // llist_for_each_entry(pdp, &mm_ctx->pdp_list, list) {
+       //      LOGMMCTXP(LOGL_INFO, mm_ctx, "Changing GTP-U endpoints %s -> %s\n",
+       //                sgsn_gtp_ntoa(&pdp->lib->gsnlu), inet_ntoa(sgsn->cfg.gtp_listenaddr.sin_addr));
+       //      sgsn_pdp_upd_gtp_u(pdp,
+       //                         &sgsn->cfg.gtp_listenaddr.sin_addr,
+       //                         sizeof(sgsn->cfg.gtp_listenaddr.sin_addr));
+       // }
 }
```

It is a dirty hack (which might not be the hack, I need to experiment more to prove that it really solves the problem), need to investigate further and get to know the reason of a problem to come up with a normal solution.

#20 - 04/18/2019 02:03 PM - efistokl

- File experiment-thu-18-4-19-2.zip added

efistokl wrote:

> So that Update PDP Context Request wasn't sent to GGSN and the PDP context didn't get deleted a moment later (due to sending "Error Indication").

Hmm, this time all went OK (experiment-thu-18-4-19-2.zip)... (without the change above) A bit confused now.

In the traces in after-patch-gerrit-13654.zip we see sgsn hard-dropping PDP ctx without sending Deactivate PDP Context Request to the UE. Hence, the UE doesn't know that PDP was deleted... But here it didn't happen...

Files

iphone-6s-osmocom.pcap	2.08 MB	04/12/2019	efistokl
iphone-6s-q.pcap	6.31 MB	04/12/2019	efistokl
sgsn-10.0.3.19.logs.txt	115 KB	04/15/2019	efistokl
iphone-6s-osmocom-10.0.3.19.pcap	1.26 MB	04/15/2019	efistokl
after-patch-gerrit-13654.zip	925 KB	04/16/2019	efistokl
experiment-thu-18-4-19.zip	594 KB	04/18/2019	efistokl
experiment-thu-18-4-19-2.zip	1.29 MB	04/18/2019	efistokl