OsmoGGSN (former OpenGGSN) - Bug #3914

PAP PCO not handled correctly

04/10/2019 05:56 AM - laforge

Status:	Resolved	**Start date:**	04/10/2019
Priority:	Normal	**Due date:**	
Assignee:	pespin	**% Done:**	100%
Category:	openggsn		
Target version:			
Spec Reference:			

Description

I don't have a GTP trace, but the attached Gb interface trace shows the following oddities:

- The PCO as sent by the MS/UE in the PDP CTX ACT REQ contains a PAP Auth Req
  - This Auth Req is malformed according to the wireshark dissector (can we trust it?), but that's not the main point here
- The PCO as returned by the network to te MS doesn't contain any PAP Auth Resp
  - not sure if support for PAP is required, but TS 24.008 at least states:
    - *At least the following protocol identifiers (as defined in RFC 3232 [103]) shall be supported in this version of the protocol:C021H (LCP); C023H (PAP); C223H (CHAP);and 8021H (IPCP).*
  - Instead, our PCO response contains **twice** the PCO for IPCP (DNS servers), which clearly is wrong

History

#1 - 04/10/2019 07:43 AM - laforge

Note that the PAP inside the capture is clarly invalid as per specification. It sends a Peer-Id-Length of 04, but there's 6 (excluding NUL byte) or 7 (including NUL byte) characters of Peer Identifier.

Nevertheless, OsmoGGSN should handle this somewhat intelligently, e.g. by sending an ACK in return.

Under no circumstances should OsmoGGSN send duplicate DNS PCOs

#2 - 04/10/2019 08:53 AM - laforge

- Status changed from New to In Progress

- % Done changed from 0 to 30

Note that the PAP inside the capture is clarly invalid as per specification. It sends a Peer-Id-Length of 04, but there's 6 (excluding NUL byte) or 7 (including NUL byte) characters of Peer Identifier.

Nevertheless, OsmoGGSN should handle this somewhat intelligently, e.g. by sending an ACK in return.

Under no circumstances should OsmoGGSN send duplicate DNS PCOs

See https://gerrit.osmocom.org/#/c/osmo-ttcn3-hacks/+/13563 for improving our TTCN3 tests to avoid duplicate PCO protocolIDs and https://gerrit.osmocom.org/#/c/osmo-ttcn3-hacks/+/13564 for a test case reproducing exactly the PCOs as observed by that phone.

#3 - 04/10/2019 01:55 PM - laforge

- % Done changed from 30 to 60

I just pushed a series of patches, and https://gerrit.osmocom.org/#/c/osmo-ggsn/+/13570 is removing the duplicate PCO response from osmo-ggsn.

we still don't have any PAP handling.

#4 - 04/11/2019 05:35 PM - laforge

See https://gerrit.osmocom.org/#/c/osmo-ggsn/+/13608 for the patch adding minimalistic PAP support. Hopefully this will make some modems happy.

#5 - 04/11/2019 05:35 PM - laforge

- % Done changed from 60 to 90

#6 - 06/26/2019 12:57 PM - pespin

I can take over this one and finishing polishing the patch if you want.

#7 - 06/27/2019 12:40 AM - laforge

On Wed, Jun 26, 2019 at 12:57:33PM +0000, pespin [REDMINE] wrote:

> I can take over this one and finishing polishing the patch if you want.

Hi Pau, if it is relatively quick to resolve: Thanks. Particularly during my holidays
I wouldn't expect me to find time for anything but the most urgent isuses :/

#8 - 06/27/2019 09:42 AM - pespin

- Assignee changed from laforge to pespin

#9 - 06/27/2019 02:17 PM - pespin

- Status changed from In Progress to Feedback

Submitted improved osmo-ggsn patches + new patches improving related code:
Updated Changes:
https://gerrit.osmocom.org/c/osmo-ggsn/+/13608 ggsn: Add minimalistic PAP support
https://gerrit.osmocom.org/c/osmo-ggsn/+/13609 ggsn: More logging from PCO handling (e.g. in case of malconfiguration)
New Changes:
https://gerrit.osmocom.org/c/osmo-ggsn/+/14619 ggsn: Avoid unaligned mem access reading PCO proto id
https://gerrit.osmocom.org/c/osmo-ggsn/+/14620 ggsn: Use structures instead of raw arrays when parsing ipcp_hdr

osmo-ttcn3 patch was also updated:
https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/13564 ggsn: Add TC_pdp4_act_deact_ipcp_pap_broken()

Once merged we can close this ticket.

#10 - 07/01/2019 10:31 AM - pespin

ggsn patches merged, osmo-ttcn3 hacks still in gerrit waiting for review. Once merged ticket can be closed.

#11 - 07/03/2019 04:25 PM - pespin

- Status changed from Feedback to Resolved

- % Done changed from 90 to 100

Merged, closing.

#12 - 07/04/2019 06:46 AM - fixeria

Thanks a lot for working on this!

With the recent OsmoGGSN I've finally managed to 'attach' my POS terminal that I had with me at OsmoDevCon 2018. What I find funny is that I already tried to make OsmoGGSN send PAP Auth ACK before, but I didn't work. My implementation was missing the welcome text , and this seems to be the key.

Files

act_pdp_req_with_pap.pcapng	792 Bytes	04/10/2019	laforge