OsmoSGSN - Bug #1794

support random IV for GEA (via XID)

08/09/2016 02:21 PM - msuraev

Status:	Stalled	**Start date:**	08/09/2016
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	10%
Category:			
Target version:			
Spec Reference:			

Description

Current implementation of GPRS encryption uses hardcoded IV = 0 while according to spec it should be random. This random value is communicated to client as part of XID negotiation.

Related issues:

Related to libosmocore - Feature #1910: add v4 encryption support	**Stalled**	**01/11/2017**
Related to OsmocomBB - Feature #1672: add gprs decoding utility	**Closed**	**03/24/2016**
Related to OsmoGGSN (former OpenGGSN) - Bug #2843: crash by icmpv6 message	**Resolved**	**01/19/2018**
Blocked by OsmoSGSN - Feature #1580: IP header compression	**Closed**	**02/23/2016**
Blocks OsmoSGSN - Bug #1582: GEA Encryption is missing	**Resolved**	**02/23/2016**

History

#1 - 08/09/2016 02:22 PM - msuraev

- Blocked by Feature #1580: IP header compression added

#2 - 08/09/2016 02:24 PM - msuraev

- Blocks Bug #1582: GEA Encryption is missing added

#3 - 08/27/2016 09:15 AM - laforge

The LLC XID related patch was just merged, so this should be possible to
implement now.
--
- Harald Welte <laforge@gnumonks.org> http://laforge.gnumonks.org/
==========
"Privacy in residential applications is a desirable marketing option."
(ETSI EN 300 175-7 Ch. A6)

#4 - 10/11/2016 09:59 AM - laforge

- Assignee set to msuraev

#5 - 11/09/2016 09:23 AM - laforge

- Priority changed from Low to High

#6 - 11/24/2016 02:02 PM - msuraev

- Status changed from New to In Progress

- % Done changed from 0 to 10

#7 - 12/05/2016 12:41 PM - msuraev

- Status changed from In Progress to Stalled

#8 - 01/12/2017 08:19 PM - laforge

- Priority changed from High to Normal

#9 - 05/23/2017 01:57 PM - laforge

ping?

#10 - 10/11/2017 08:26 AM - laforge

another ping, 5 months later. This is not acceptable.

#11 - 10/11/2017 11:51 AM - msuraev

Sorry, completely slipped of my mind - I was sure I've updated it. There's incomplete implementation in gerrit 1462 which is not working unfortunately: we send IV to the phone, we got encrypted traffic back but we fail to decrypt it (using IV we've sent or IV=0). Which means that the phone interprets it somehow differently. To debug this we've got to somehow get phone's baseband logs. Unfortunately xgoldmon and osmocom-bb do not support gprs yet. Not sure if there's better way to see what goes wrong.

#12 - 01/15/2018 11:24 AM - msuraev

- Status changed from Stalled to In Progress

The patch is ported to OsmoSGSN and available in gerrit 5788. It still requires further testing and adjustements before in can be merged though.

#13 - 01/22/2018 12:33 PM - msuraev

- Related to Feature #1910: add v4 encryption support added

#14 - 01/22/2018 04:52 PM - msuraev

- Related to Feature #1672: add gprs decoding utility added

#15 - 01/22/2018 04:53 PM - msuraev

- Related to Bug #2843: crash by icmpv6 message added

#16 - 01/30/2018 09:17 AM - msuraev

- Status changed from In Progress to Stalled

#17 - 03/01/2018 11:17 PM - laforge

- Assignee deleted (msuraev)