Cellular Network Infrastructure - Bug #3043

A5/3 encryption fails

03/08/2018 10:15 AM - jbruckner

Status:	Resolved	**Start date:**	03/08/2018
Priority:	High	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

This was discussed a bit on the mailing list already: http://lists.osmocom.org/pipermail/openbsc/2018-March/011811.html

I'm attaching the Wireshark traces from the mails. Please see the respective mail from the archive for a description of what has been recorded there.

Here's my initial mail:

I'm having trouble using the A5/3 encryption in my setup. A5/1 works perfectly fine [attachment a5_1.pcapng]. As soon as I switch to A5/3 and e.g. send an SMS, the last valid message I see in the Wireshark traces of the GSMTAP of osmo-bts-trx is the Ciphering Mode Command requesting A5/3. After that, several messages arrive at the bts, but it seems like it can't make any sense of them. The MS repeatedly tries to send the SMS but never succeeds [attachment a5_3.pcapng]. Both MSs are connected to the same bts.

According to the Classmarks of all MSs, A5/1 as well as A5/3 are supported.
This is my Setup:
- USRP N210
- osmo-trx
- osmo-bts-trx
- osmo-nitb
- osmo-pcu
- osmo-sgsn
- osmo-ggsn

I'm using a Debian 9 VM and tried both the packages from osmocom-latest as well as osmocom-nightly.
The MSs I've tested are two Nexus 6 and one Samsung Galaxy S I9000. All three with sysmocom nano USIMs.

Could the decryption at the bts be incorrect? Has anyone tested/used it recently?
I'll be happy to provide additional information if needed.

Related issues:

Related to OsmoBSC - Bug #3183: BSC_Tests.ttcn lacks tests for BSSMAP Cipher ...	**Resolved**	**04/18/2018**
Related to OsmoBTS - Bug #3184: BTS_Tests.ttcn is lacking test for encryption	**Resolved**	**04/18/2018**
Related to OsmoMSC - Bug #2947: OsmoMSC crashes with A5/3 configured and MS s...	**Resolved**	**02/15/2018**
Related to OsmoBSC - Bug #3186: cipher mode reject may be sent with invalid c...	**Resolved**	**04/19/2018**
Related to OsmoMSC - Bug #3187: rx cipher mode reject from BSS broken	**Closed**	**04/19/2018**
Related to OsmoMSC - Feature #2795: Handle UTRAN_CLSM_CHG in MSC	**New**	**12/29/2017**
Related to OsmoGSMTester - Feature #3563: osmo-gsm-tester: add test case: tes...	**Resolved**	**09/18/2018**

History

#1 - 04/18/2018 01:21 PM - jbruckner

- File a5_3_Cipher_Mode_Reject.txt added

Attaching log from the MSC as described on the mailing list.

#2 - 04/18/2018 02:57 PM - laforge

pespin: Is osmo-gsm-tester testing with different encryption settings? If not, I think it would be a rather easy-to-do but important improvement if we'd

have at least one test in each current-day encryption mode (a5/0, a5/1, a5/3). In the end, it's the same test case, just running with one modified field in the config file.

jbruckner: What we're testing on the BSC level is:

- BSC_Tests.TC_assignment_fr_a5_0
- BSC_Tests.TC_assignment_fr_a5_1
- BSC_Tests.TC_assignment_fr_a5_3
- BSC_Tests.TC_assignment_fr_a5_4

so we're quite confident the BSC is doing what it's supposed to do, if it receives a related ASSIGNMENT CMD from the MSC.

On the MSC sidde, we have

- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_013_2
- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_13_13
- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_13_2
- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_1_13
- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_3_1
- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_3_13
- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_3_1_log_msc_debug
- MSC_Tests.TC_lu_imsi_auth_tmsi_encr_3_1_no_cm

So we're equally sure that the selection of the right encryption algorithm is performed as intended.

What's missing are tests for

- BSC in non-assignment case (ciphering mode)
- BTS tests for both assignment and non-assignment cases

I'll add separate tickets for the missing TTCN-3 tests

#3 - 04/18/2018 03:10 PM - laforge

- Related to Bug #3183: BSC_Tests.ttcn lacks tests for BSSMAP Cipher Mode Control added

#4 - 04/18/2018 03:12 PM - laforge

- Related to Bug #3184: BTS_Tests.ttcn is lacking test for encryption added

#5 - 04/19/2018 12:47 PM - neels

- Related to Bug #2947: OsmoMSC crashes with A5/3 configured and MS sending no Classmark 2 in LU Request added

#6 - 04/19/2018 12:52 PM - neels

We still have a problem with A5/3, namely that the indication whether A5/3 is supported is not contained in the classmark IE received upon Location Updating. Recently, a code change was introduced that ensures the ciphering we initiate is indeed supported by the MS, which of course denies A5/3 if we don't have the information that A5/3 is indeed supported.
http://git.osmocom.org/osmo-msc/commit/?id=71330720b6efdda2fcfd3e9c0cb45f89e32e5670

What is needed here is that the MSC sends a Classmark Request to the BSS, so that we will subsequently receive a Classmark Update containing the A5/3 support indicator.

In practice, we have thus broken A5/3 until this gets implemented. This was mentioned in issue #2947, but I notice now that unfortunately the Classmark Request part was lost in resolving the segfault part.

Thanks for re-raising this.

#7 - 04/19/2018 01:14 PM - neels

- Related to Bug #3186: cipher mode reject may be sent with invalid cause code added

#8 - 04/19/2018 01:15 PM - neels

- Related to Bug #3187: rx cipher mode reject from BSS broken added

#9 - 04/20/2018 10:30 AM - laforge

On Thu, Apr 19, 2018 at 12:52:14PM +0000, neels [REDMINE] wrote:

> What is needed here is that the MSC sends a Classmark Request to the BSS, so that we will subsequently receive a Classmark Update containing the A5/3 support indicator.

this is **only** required if the MS is not sending the CLASSMARK CHANGE anyway, which 99.9% of the phones do.

> In practice, we have thus broken A5/3 until this gets implemented. This was mentioned in issue #2947, but I notice now that unfortunately the Classmark Request part was lost in resolving the segfault part.

Are you sure that it fails even when CLASSMARK CHANGE is received from the phone? it contains CM3.

#10 - 04/23/2018 09:57 PM - neels

I can say for sure that the Samsung S4mini wasn't able to subscribe with A5/3.
IIRC we fail to accept the Classmark Update while the conn is still being established. Need to test for specific details...
I dimly remember to have opened an issue to accept that in osmo-msc, but can't seem to find it anymore (edit: #2795)

(btw, about the naming, it seems to be a CLASSMARK CHANGE on Abis, and Classmark Update on BSSMAP)

#11 - 04/24/2018 06:19 AM - laforge

On Mon, Apr 23, 2018 at 09:57:38PM +0000, neels [REDMINE] wrote:

> (btw, about the naming, it seems to be a CLASSMARK CHANGE on Abis, and Classmark Update on BSSMAP)

yes. That's why it makes sense to always prefix with the protocol, such
as "RR CLASSMARK CHANGE". RR CLASSMARK CHANGE can happen both as unidirectional
un-solicited report by the MS, as well as in response to a RR CLASMARK ENQUIRY by
the BSC.

#12 - 04/30/2018 12:06 PM - neels

- Related to Feature #2795: Handle UTRAN_CLSM_CHG in MSC added

#13 - 08/08/2018 11:15 AM - laforge

- Assignee set to neels

- Priority changed from Normal to High

#14 - 09/13/2018 03:28 AM - neels

- Status changed from New to In Progress

- % Done changed from 0 to 50

First off, implemented the RR Classmark Enquiry to be sent by osmo-bsc: https://gerrit.osmocom.org/#/c/osmo-bsc/+/10910

Got working patches for osmo-msc that sends a BSSMAP Classmark Request to the BSC, waits for BSSMAP Classmark Update and thus figures out whether A5/3 is available; patches still needs grooming; osmo-msc.git branch neels/a53

After that I want to investigate early classmark, i.e. that we don't actively need to request CM3 but the MS/UE sends it unasked and right away.

#15 - 09/13/2018 03:33 AM - neels

ah yes, and it's only working for vlr_lu_fsm so far, vlr_proc_acc_req FSM for CM Service and Paging Response needs similar changes.

#16 - 09/14/2018 08:11 PM - neels

Actually, for A5/3, Classmark 2 indicates MS support for it, which is always mandatory for both CM Service Request as well as Paging Response. So, for A5/3, we will require asking for a Classmark Update **only** during LU, never during CM Service Req or Paging Response.

#17 - 09/17/2018 12:15 AM - neels

- % Done changed from 50 to 80

https://gerrit.osmocom.org/10985 ensures that we keep Classmark information in the VLR, i.e. across conns.

https://gerrit.osmocom.org/10987 implements Classmark Request for all Ciphering code paths where a Classmark with the appropriate A5/n support indicator is missing.

Haven't checked early classmark sending yet.

#18 - 09/18/2018 11:57 AM - pespin

- Related to Feature #3563: osmo-gsm-tester: add test case: test a5/3 added

#19 - 09/18/2018 12:54 PM - neels

- % Done changed from 80 to 90

Early Classmark Sending is already configurable in osmo-bsc config: 'bts 0' / 'early-classmark-sending (allowed|forbidden)'.
The default is currently 'forbidden'. I would have changed that to 'allowed' if that didn't silently change existing users' configuration.

The osmo-msc patches are already merged, A5/3 will work as soon as the osmo-bsc ones are merged:

osmo-bsc implementation of Classmark Enquiry: https://gerrit.osmocom.org/c/osmo-bsc/+/10910
ttcn3 test for Classmark Enquiry: https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/11012

#20 - 09/24/2018 05:12 PM - fixeria

I think the reason of this issue may be actually described in #3253, which was fixed by Harald
(see https://git.osmocom.org/osmo-bts/commit/?id=e152fd2614a2159f2918d2ac721793856ca4d873).

#21 - 09/25/2018 08:37 AM - neels

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

fixeria wrote:

> I think the reason of this issue may be actually described in #3253

At least one reason was that the MSC refused to enable A5/3 in the lack of Classmark 2.
If there is an A5/3 issue with osmo-bts-trx, then it's completely independent from this one.

osmo-msc, osmo-bsc patches are merged.

#22 - 09/25/2018 09:27 AM - jbruckner

Thanks for working in this! Since the status is now 100% should I test again with the next nightly builds?

#23 - 09/25/2018 11:35 AM - neels

Yes, give it a spin, I am expecting success. Should it still fail, we need to re-open this issue. Thanks!

#24 - 01/14/2019 02:35 PM - jbruckner

I finally got around to testing it. I can confirm A5/3 is now working :)
Thank you for fixing this!

#25 - 01/15/2019 02:19 PM - neels

yw =)

Files

a5_1.pcapng	11.4 KB	03/08/2018	jbruckner
a5_1_3_with_LU_Auth.pcapng	94.1 KB	03/08/2018	jbruckner
a5_3.pcapng	68 KB	03/08/2018	jbruckner
attach_a5_0_1_3.pcapng	85.6 KB	03/08/2018	jbruckner
a5_3_Cipher_Mode_Reject.txt	7.1 KB	04/18/2018	jbruckner