OsmoGSMTester - Support #2497

Set up SIM cards with auth algo other than comp128v1

09/06/2017 03:16 PM - neels

Status:	Stalled	**Start date:**	09/06/2017
Priority:	Normal	**Due date:**	
Assignee:	daniel	**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

It appears all SIM cards currently in the osmo-gsm-tester rnd and prod setup are configured to use XOR auth.

(Edited)

We saw auth failing, but succeeding when setting the HLR to XOR.
XOR is currently not available, and the only reason that choosing XOR would lead to success is that the HLR does not provide any auth data and the MSC continues **without** authentication.

For authentication related test runs, we need to set 'network' / 'authentication required' in the osmo-msc.cfg,
and we should probably also set 'encryption a5 3' to see that the negotiated kc works for encryption.

We do not support XOR, and we should have more diverse auth algos in place.
Best would be one using Milenage (the 2G variant), one using comp128v1, one using comp128v3.

We then need to adjust the resources.conf and can set up different auth tests for the various algos.

Related issues:

Related to libosmocore - Feature #2475: XOR authentication not implemented	**Resolved**	**08/31/2017**

History

#1 - 09/06/2017 03:21 PM - neels

The important part is that we test both UMTS auth = 2G-Milenage, as well as the old GSM plain way, say comp128v3.
If comp128v3 works in the osmo-gsm-tester and the other algos pass the 'make check' tests, there is no reason why those should fail in the osmo-gsm-tester.

Note: the 2G-Milenage will only work with the new VLR, i.e. only in the AoIP tests.

#2 - 09/06/2017 04:54 PM - laforge

I would argue we should ideally test:

- 2G auth with classic 2G algorithm (COMP128x) over 2G bearer
- 2G auth with classic 2G algorithm (COMP128x) over 3G bearer, i.e. SIM Card with no UICC application present (sysm-usim-util can remove it)
- 3G auth with MILENAGE over 3G bearer
- 2G auth derived from MILENAGE over any bearer (shouldn't matter).

I'm not sure if this must be done as part of osmo-gsm-tester, as
(without using remote sim features) we cannot easily swap sim cards
and/or reprogram them on the fly.

This should be possible to test with osmo-bts-virtual + osmocom-bb, or
even by some more direct way where a small sim-card using utility
program talks BSSAP to the MSC. Whatever is the method of least effort.

BTS+BSC have no influence on the authentication, it's all in
MSC/VLR/HLR, so I don't think it's important to do this over real or
virtual radio interface.

Regarding 3G bearer: Do we yet have tickets for osmo-gsm-tester to
include 3G support testing with e.g. nano3G + osmo-hnbgw ?

#3 - 09/07/2017 04:57 AM - neels

laforge wrote:

> I would argue we should ideally test:

[...]

> I'm not sure if this must be done as part of osmo-gsm-tester, as

ok, so having XOR in the gsm-tester doesn't matter?
I think I'd like to have at least a little diversity in auth algos there, because we can.

> Regarding 3G bearer: Do we yet have tickets for osmo-gsm-tester to
> include 3G support testing with e.g. nano3G + osmo-hnbgw ?

no, and no focus on that so far, but makes sense increasingly. Let's get settled with the new repositories first and take it from there...

#4 - 09/07/2017 07:36 AM - laforge

Hi Neels,

On Thu, Sep 07, 2017 at 04:57:56AM +0000, neels [REDMINE] wrote:

> > I'm not sure if this must be done as part of osmo-gsm-tester, as
>
> ok, so having XOR in the gsm-tester doesn't matter?

I don't think so, at least for sure not if we implement related testing
by some other means. As indicated, only SIM card and MSC+HLR (or:
SGSN+HLR) are involved in this anyway. It should be rather simple to
"fake" a LU / IMSI ATTACH on the A, Iu or Gb interface to trigger related
authentication transaction from a machine with a few SIM card readers
attached. This looks much easier to really test all relevant
configurations than exploding the number of (lengthy) tests on osmo-gsm-tester
and to add so many different SIM variants + related modems.

> I think I'd like to have at least a little diversity in auth algos there, because we can.

Sure, if you'd like and if it doesn't significantly complicate the setup or configuration?

#5 - 09/07/2017 09:22 AM - pespin

> > I think I'd like to have at least a little diversity in auth algos there, because we can.
>
> Sure, if you'd like and if it doesn't significantly complicate the setup or configuration?

It should work transparently as we already have support to subscribe each modem based on its auth algo set in the configuration file. We can even pick a modem based on its auth algo configured in the SIM card. So it's mostly spending time on changing the SIM information (never done that but I've been told is easy), then we test them for free with other tests, even if we don't spend time testing the feature explicitly.

#6 - 12/14/2017 11:14 AM - daniel

- Related to Feature #2475: XOR authentication not implemented added

#7 - 12/14/2017 01:16 PM - neels

- Description updated

#8 - 10/25/2018 06:22 PM - laforge

- Assignee changed from osmo-gsm-tester to pespin

what's the status here?

#9 - 10/26/2018 04:56 PM - pespin

We are currently using algo "comp128v1" for all modems. Configuring each subscriber to use another algo in osmo-gsm-tester only requires a one-line change for each subscriber/modem in the config file.
I'm not sure if then we also require to change the SIMcard config. If that's the case, someone with physical access to the setup needs to take care of that part.

#10 - 10/29/2018 02:35 PM - neels

This issue came about due to mismatching enum values for the auth algos, so that it looked in the logs like the tester would use XOR, while the cards were in fact using COMP128vN all the time. The XOR part of this issue is moot.

To have diverse auth algos, we need to program the SIM cards in the hardware setup. If we want that. We probably do want that, but it's not super urgent, is it.
I'd suggest testing at least COMP128v3 and UMTS Milenage (yes, on GSM), maybe also COMP128v1

#11 - 10/29/2018 02:49 PM - pespin

WE should then assign this ticket to somebody who can program the simcards in there. Once that's done, I can change the config in osmo-gsm-tester to use the new algo.

#12 - 10/29/2018 11:30 PM - laforge

If the modems suport AT+CSIM or +CRSM it may even be possible to do any reprogramming "live"
while the cards are still in the modems. But I guess, if at all, we should invest time
into using "remote" SIM cards at that point.

#13 - 11/01/2018 02:10 PM - pespin

- Status changed from New to Feedback

- Assignee changed from pespin to laforge

I'm not sure how to proceed with this task then. Can we decide what do we want to do? I thought someone had to flash the simcard physically to change the IMSI, but if it can be done through the modem, I can then investigate that.

So let's take one of the 3 possibilities:
A- Investigate how to change algo parameters through modem AT commands (then assigned to me or someone else as we see).
B- Program simcards using pySim or whatever, then issue needs to be assigned to somebody with physical access to simcards
C- Setup remoteSim setup for the modems. I guess in first place we require some HW setup, so then this task should be assigned to somebody else.

#14 - 01/03/2019 02:39 PM - laforge

- Status changed from Feedback to Stalled

- Assignee changed from laforge to daniel

pespin wrote:

> So let's take one of the 3 possibilities: [...]
>
> B- Program simcards using pySim or whatever, then issue needs to be assigned to somebody with physical access to simcards

Ok, then let's go for this. daniel, please take care of this, coordinating with pespin to ensure the cards are changed at the same time as the configuration files of osmo-gsm-tester are changed.

#15 - 10/15/2019 11:44 AM - daniel

- Subject changed from Set up SIM cards with auth algo other than XOR to Set up SIM cards with auth algo other than comp128v1

Ok, so to summarize:

- All cards in osmo-gsm-tester are using comp128v1 at the moment
- We want to test different auth algos - comp128v1, v3 and milenage (for 2G and 3G?)
- 3G auth support in osmo-gsm-tester is not present (the HLR auc_3g table is never populated)

If someone points me to the card in the osmo-gsm-tester (or tells me which imsi to look for) I can change the auth algo and also program in a K/OPC.