OsmoNITB - Feature #1711

Feature # 1595 (Closed): Addition of an Iu-CS interface

3G Auth

05/14/2016 12:06 AM - neels

Status:	Closed	**Start date:**	05/14/2016
Priority:	Urgent	**Due date:**	
Assignee:	neels	**% Done:**	100%
Category:			
Target version:	Asynchronous HLR+AUC for CS		
Spec Reference:			

Description

Related issues:

Related to OsmoNITB - Feature #1592: VLR in libmsc, to connect to HLR asynchr...	**Closed**	**02/23/2016**
Related to OsmoNITB - Feature #1593: UMTS AKA support	**Closed**	**02/23/2016**
Related to Cellular Network Infrastructure - Support #1965: use sysmoUSIM-SJS...	**Closed**	**03/04/2017**

History

#1 - 05/14/2016 12:06 AM - neels

- Related to Feature #1592: VLR in libmsc, to connect to HLR asynchronously added

#2 - 05/14/2016 12:07 AM - neels

so far hardcoded 2G KI are used on the sysmocom/iu branch

#3 - 08/01/2016 12:23 PM - laforge

- Related to Feature #1593: UMTS AKA support added

#4 - 08/01/2016 12:23 PM - laforge

- Assignee set to laforge

#5 - 08/09/2016 12:15 PM - laforge

- Priority changed from Normal to Urgent

#6 - 11/11/2016 08:38 AM - laforge

- Assignee changed from laforge to neels

#7 - 11/24/2016 04:42 PM - neels

Started off by a small detour: write python code to produce dotty graphs
from osmo_fsm C code.

https://git.osmocom.org/libosmocore/log/?h=neels/fsm-to-dot
temporary example upload: http://kleinekatze.de/quooXai5/

Writing this first off helped in understanding how these structures are built,
and the graphs will help tremendously during further development.

#8 - 12/02/2016 05:16 PM - laforge

- Target version set to Asynchronous HLR+AUC for CS

#9 - 12/06/2016 12:20 PM - neels

- Status changed from New to In Progress

#10 - 01/10/2017 12:57 PM - neels

- % Done changed from 0 to 50

The VLR integration work is tracked in #1592. So when that is done and the 3G branch gets rebased onto it, this issue's progress will probably jump to 100%. So let me set it to 50% for now, showing that things are in progress.

#11 - 01/23/2017 11:50 AM - wirelesss

#12 - 02/02/2017 03:11 AM - neels

- % Done changed from 50 to 60

On the vlr branch, the first end-to-end test for UMTS milenage authentication is in place
and working, though still lacking the milenage sequence nr synchronisation procedure,
and not tested with real equipment yet.

Done:

- MM Auth Request composition and Response parsing were extended to accomodate UMTS extensions.
- the VLR now detects whether a subscriber connection is via UTRAN or GERAN
- and whether the subscriber is capable of R99,
- it detects whether the HLR provided UMTS and/or GSM auth tokens and
- sends the corresponding Auth Request message.
- res/sres is parsed from the auth response in the MSC and
- the VLR verifies against the expected res/sres.

Next:

- milenage seq sync: add parsing of AUTS message, handle in VLR to re-issue Auth Request.

After that:

- more regression tests verifying graceful rejection in auth failure cases.
- test gsm-milenage, i.e. compatibility mode of milenage in a pre-R99 environment.
- try to rebase the sysmocom/iu branch onto the VLR changes to test real world 3G auth?

#13 - 02/07/2017 11:15 AM - neels

UMTS Resync: Parsing of AUTS (auth response resync token) is merged to openbsc master.
On the VLR branch, the UMTS (milenage) resync procedure is implemented and tested
across MSC, VLR and HLR (i.e. is complete).

libosmocore and osmo-hlr (as well as some docs and cmdline util) had the wrong
size for AUTS, which is now comprehensively fixed from 16 to 14 bytes:
https://gerrit.osmocom.org/#/c/1731/, #1874

Found a problem in osmo_auth_gen_vec_auts() where the API .h had different arg ordering
than the implementation. This is fixed in
https://gerrit.osmocom.org/#/c/1737/, https://gerrit.osmocom.org/1739

Clarified resync output for osmo-gen-vec in https://gerrit.osmocom.org/1734

#14 - 02/09/2017 03:26 AM - neels

A few oddities were found and fixed while writing the MSC+VLR tests for HLR rejects as described in #1922:

- don't send auth failure to HLR when the auth failure was due to the HLR not knowing the subscriber / not providing auth tuples
- proper auth reject cause if IMSI is known but no auth tuples are obtained
- auth reject logic fix in case a GSUP auth ACK contains no tuples
- introduced optional vlr->cfg.auth_tuple_max_use_count (though re-using the exact same auth tuples opens the doors for replay attacks; the default is to use once only, even on HLR error).

#15 - 02/14/2017 03:22 PM - neels

- % Done changed from 60 to 80

Verified with real equipment that our GSM-Milenage algorithm (for abbreviated Milenage on pre-R99 networks)
works with a sysmoUSIM-SJS1 configured to do Milenage for both 2G and 3G.

One thing though, I expected this to now do full UMTS Auth when using an R99+ MS, and the GSM-Milenage fallback
only when the MS is pre-R99. But even though the USIM is in an R99+ MS (Samsung Galaxy S4m), the LU Request still

indicates "GSM phase 2" in the classmark and GSM-Milenage is used instead of normal UMTS Milenage.

Is there something else we can set on the USIM to make it show as R99 on the GSM network?
(It does show as R99 on a 3G network.)

#16 - 02/28/2017 02:23 AM - neels

- % Done changed from 80 to 90

neels wrote:

> Is there something else we can set on the USIM to make it show as R99 on the GSM network?
> (It does show as R99 on a 3G network.)

As described elsewhere, this was due to the MSCR in SI3 being 0, indicating a pre-R99 MSC.
Full UMTS AKA has been verified to work with a USIM on a GSM network (with MSCR set to 1),
with real equipment.

All that would be missing now is a rebase of the 3G work onto the VLR work and a test of UMTS AKA on UTRAN.

#17 - 03/01/2017 04:41 PM - neels

Started to rebase the sysmocom/iu branch onto the neels/vlr branch.
The first conflict resolution is done, but I need to re-check pretty much every detail,
to make sure nothing got lost.

Rebasing a long branch like this is not very efficient -- a given resolved conflict potentially re-appears N times, e.g. if a given section was deleted, and the branch edits that section in N separate commits. Each edit brings back the same conflict and the given section has to be removed again each time.

It might make sense to collapse the Iu branch into one code bomb commit to cut short future rebases, but then I might have to re-untangle the spaghetti later for code review by others.

An alternative is to merge instead of rebasing, but that will make the history less linear once things get merged to master. I'd prefer to avoid that confusion.

I will see how it goes on, for now amending / purging the individual iu patches to make sense with the new VLR auth, hoping that most of these conflicts are done now anyway and won't re-appear; but if I continue to spend time in rebase conflicts I will reconsider.

#18 - 03/01/2017 08:18 PM - laforge

On Wed, Mar 01, 2017 at 04:41:46PM +0000, neels [REDMINE] wrote:

> Rebasing a long branch like this is not very efficient [...]
> It might make sense to collapse the Iu branch into one code bomb commit [...]
> An alternative is to merge instead of rebasing, [...]

I'm quite flexible here, we should try to make sure you can work
efficiently.

#19 - 03/03/2017 03:26 AM - neels

All conflicts have been resolved.
The combined code compiles.
All tests pass, including msc_vlr end-to-end tests, notably some running for RAN_GERAN_A and some for RAN_UTRAN_IU.

The function to transmit over A-interface, a_tx() (vs. iu_tx()), is of course not implemented yet,
but the msc_vlr tests override it to evaluate what messages *would* be sent over the A-interface.
Also added an a_page() function (vs. iu_page_cs()) for the same purpose.

Added a vlr_subscr->cs.via_ran indicator to remember which RAN it attached over, mostly to know which way to send Paging,
to a_page() or iu_page_cs(). This will probably change when we enhance OsmoMSC Paging to use the LAC.
Added a check that prevents mixing RAN types (not sure about 2G/3G handover, but for now mixing is prohibited).

Next up:

- actual tests with the nano3G, sysmoUSIMs and Galaxy phones
- check for important FIXMEs and errors
- fixup / collapse commits, obliterate scores of dead code

#20 - 03/04/2017 03:21 AM - neels

- Status changed from In Progress to Resolved

- % Done changed from 90 to 100

The rebased iu-onto-vlr branch works with real USIM on real nano3G!
Both OsmoMSC and OsmoSGSN authenticate the USIM via real IuCS+IuPS using the new OsmoHLR, using milenage successfully!
This is a major milestone, I'm quite satisfied right now.

The sysmocom/iu branch as of now includes the VLR branch, talks to OsmoHLR and is capable of full UMTS Authentication.
Some code cleanup is pending, but that's not of concern to this 3G Auth issue.

Notably: it works well with the USIM that dexter programmed to use Milenage on both 2G and 3G,
but another unchanged sysmoUSIM keeps failing to authenticate. It does an AUTS resync which seems to not work out.
I tried setting other algos in the HLR, they are all rejected with "GSM auth not acceptable" or the HLR errors out.
So the accelerate3g5 guys may have to reprogram their USIMs to EF.AUTH = 0101 like the one I got from dexter.
I'll investigate further in another ticket: #1965

#21 - 03/04/2017 05:29 AM - neels

neels wrote:

> The rebased iu-onto-vlr branch works with real USIM on real nanoBTS!

Typo! nano3G!!

#22 - 03/08/2017 10:08 PM - laforge

- Related to Support #1965: use sysmoUSIM-SJS1 with 3G OsmoMSC added

#23 - 04/25/2017 01:57 PM - laforge

- Status changed from Resolved to Closed