Cellular Network Infrastructure - Feature #3733

Send IMEI from MSC to HLR

12/14/2018 02:17 PM - osmith

Status:	Resolved	**Start date:**	12/14/2018
Priority:	Normal	**Due date:**	
Assignee:	osmith	**% Done:**	100%
Category:			
Target version:			
Spec Reference:			

Description

We want to store the IMEI in HLR (see OS#2541). But first, we need to send it from the MSC to the HLR.

laforge wrote:

> Some context:
>
> - Normally, a HLR doesn't store IMEI information, rather the EIR (Equipment Identity Register) does
> - The VLR in the MSC will explicitly issue a CHECK_IMEI procedure, which will send a MAP request to the EIR and ask if this IMEI is permitted or not
> - The EIR will respond to the VLR
>
> The purpose of this procedure as per 3GPP specs is to have a blacklist/whitelist of IMEIS that is pre-populated using out-of-band sources. It is **not** to dynamically store information about IMEIS.
>
> While we use GSUP and not MAP, we still want to have the same abstract trasactions, procedures and message flows. This means, we have to implement whatever the MAP CHECK IMEI procedure normally does, but then OsmoHLR can, optionally, if enabled by VTY, store the received IMEI information in some table. So rather than a policy check, it would be used for dynamically storing the IMEI/IMSI mappings as they appear over time.

So far, the VLR/MSC is able to query the IMEI from the MS.

This issue is about implementing and using the CHECK_IMEI related messages in GSUP, based on the MAP spec 29.002 (see 25.6 IMEI Handling Macros).

The EIR (Equipment Identity Register) part that would usually report if a device is stolen or not, will be implemened in osmo-hlr and always accept all incoming IMEIs.

Related issues:

Related to OsmoHLR - Feature #2541: have IMEI in HLR DB	**Resolved**	**10/06/2017**
Related to OsmoMSC - Feature #3189: make retrieval of IMEI configurable	**Resolved**	**04/19/2018**

History

#1 - 12/14/2018 02:17 PM - osmith

- Related to Feature #2541: have IMEI in HLR DB added

#2 - 12/14/2018 02:17 PM - osmith

- Related to Feature #3189: make retrieval of IMEI configurable added

#3 - 12/19/2018 01:13 PM - osmith

- % Done changed from 0 to 10

So far I've added the GSUP messages for Check_IMEI, and successfully sent them from the MSC/VLR to HLR, and back (request and ACK). Next I

was looking into the state machine.

I was certain that I need to add it in the state machine for Process_Access_Request_VLR (vlr_access_req_fsm.c), because its header file had a PR_ARQ_S_WAIT_CHECK_IMEI state. But it did not execute any code I've added to do the Check_IMEI request when the ME connects. Later I figured out, that this was the wrong FSM, because this is only for handling "a request from the MS for access for SMS transfer or SS activity" as the spec says. After talking to neels, we decided that this is not relevant to our use case, as we want to send the IMEI to the HLR when the device first connects, not when sending SMS.

Instead, I'm looking at the Update_Location_Area_VLR FSM now, which is defined in vlr_lu_fsm.c and can be changed in vlr.c when the IMEI arrives from the MS.
Update_Location_Area_VLR only executes Check_IMEI_VLR indirectly through the Location_Update_Completion_VLR FSM (also defined in vlr_lu_fsm.c) and I'm figuring out now how to dispatch the status changes between the FSMs properly, so it matches what the spec does.

Meanwhile, I have found a completely different approach to using Check_IMEI. More recent version of the 23.012 spec have in "4.1.2.1 Process Update_Location_Area_VLR":

> The Automatic Device Detection (ADD) function is an optional feature that allows the HLR to be updated with the current User Equipment (IMEISV) and thus enables the network to configure the subscriber's equipment based on a predefined profile.

laforge, neels**: sounds like it is more suitable for what we want to do, should I look into that instead?**

I'll continue with the Check_IMEI appraoch for now, I'm learning a lot along the way and could use that to work on ADD instead if that is desired.

(EDIT: Also I found this post from 2009, where the author mentions building a IMEI<>IMSI DB based on Check_IMEI. So we might not be the only ones using this side-effect of Check_IMEI.)

EDIT2: current progress is in osmith/send-imei-to-hlr branch in osmo-hlr, osmo-msc, libosmocore.

#4 - 12/19/2018 04:10 PM - laforge

> The Automatic Device Detection (ADD) function is an optional feature that allows the HLR to be updated with the current User Equipment (IMEISV) and thus enables the network to configure the subscriber's equipment based on a predefined profile.

> laforge, neels**: sounds like it is more suitable for what we want to do, should I look into that instead?**

I think it's best to stick with check_imei as that's what's supported for decades in GSM,
without having to rely on very recent releases.

On Wed, Dec 19, 2018 at 01:13:20PM +0000, redmine@lists.osmocom.org wrote:

> Instead, I'm looking at the Update_Location_Area_VLR FSM now, which is defined in vlr_lu_fsm.c and can be changed in vlr.c when the IMEI arrives from the MS.
> Update_Location_Area_VLR only executes Check_IMEI_VLR indirectly through the Location_Update_Completion_VLR FSM (also defined in vlr_lu_fsm.c) and I'm figuring out now how to dispatch the status changes between the FSMs properly, so it matches what the spec does.

this looks good.

#5 - 12/21/2018 10:12 AM - osmith

- Checklist item [ ] libosmocore changes merge to master added
Checklist item [ ] hlr changes merge to master added
Checklist item [ ] submit msc changes to gerrit added
Checklist item [ ] msc changes merged to master added
Checklist item [ ] update wireshark GSUP protocol added
Checklist item [ ] update GSUP documentation added

Proof of concept was working yesterday, I've cleaned up the libosmocore and HLR patches and submitted them:
https://gerrit.osmocom.org/#/q/topic:send-imei-to-hlr+(status:open+OR+status:merged)

I had mostly implemented the GSUP message by reading "Procedure Check_IMEI_VLR (TS 23.018 Chapter 7.1.2.9)" and only discovered "MAP_CHECK_IMEI service 29.002 8.7.1" as I wrote the commit message, so I am not sure if this simple version is close enough to the specs. Looking forward to the review :)

In MSC, the testsuite needs to be adjusted after the changes, so patches are not submitted yet. That's what I'm working on next.

#6 - 12/21/2018 10:12 AM - osmith

- % Done changed from 10 to 30

#7 - 12/21/2018 12:48 PM - osmith

- Checklist item [x] libosmocore changes merge to master set to Done
Checklist item [x] hlr changes merge to master set to Done
Checklist item [x] submit msc changes to gerrit set to Done
Checklist item [x] update GSUP documentation set to Done

#8 - 01/08/2019 12:17 PM - osmith

- % Done changed from 30 to 60

#9 - 01/08/2019 04:09 PM - osmith

- % Done changed from 60 to 90

OsmoMSC changes pushed to Gerrit.

I've also implemented the GSUP dissector changes in Wireshark, tested them and submitted the patch:
https://code.wireshark.org/review/#/c/31445/

#10 - 01/16/2019 10:02 AM - osmith

- Checklist item [x] msc changes merged to master set to Done
Checklist item [x] update wireshark GSUP protocol set to Done

#11 - 01/16/2019 10:43 AM - osmith

- Status changed from New to Resolved

- % Done changed from 90 to 100

Done \o/