OsmoHLR - Bug #3651

SS request results in lingering lchan

10/12/2018 02:18 PM - keith

Status:	Resolved	**Start date:**	10/12/2018
Priority:	High	**Due date:**	
Assignee:	fixeria	**% Done:**	100%
Category:			
Target version:			

Description

SS codes such as *#21# are not handled correctly

Output on the HLR:

```
Fri Oct 12 14:55:26 2018 DSS <0004> hlr_ussd.c:467 262420312915730/0x20000003: Process SS (BEGIN)
Fri Oct 12 14:55:26 2018 DSS <0004> hlr_ussd.c:401 262420312915730/0x20000003: SS CompType=Invoke,
 OpCode=IngerrogateSS
```

followed by:

```
Fri Oct 12 14:55:56 2018 DSS <0004> hlr_ussd.c:195 262420312915730/0x20000003: SS Session Timeout,
 destroying
```

But osmo-bsc still has:

```
OsmoBSC# show lchan s
BTS 0, TRX 0, Timeslot 0 CCCH+SDCCH4, Lchan 0, Type SDCCH, State ESTABLISHED - L1 MS Power: 5 dBm
RXL-FULL-dl:  -47 dBm RXL-FULL-ul:  -56 dBm
OsmoBSC#
```

and this persists, with some phones, forever.

Related issues:

Related to OsmoMSC - Feature #3655: Introduce self-destruction timer for SS/U...	**Resolved**	**10/16/2018**

History

#1 - 10/12/2018 02:22 PM - keith

See also: http://lists.osmocom.org/pipermail/openbsc/2018-October/012260.html

#2 - 10/12/2018 07:51 PM - fixeria

- Project changed from Cellular Network Infrastructure to OsmoHLR

- Status changed from New to Feedback

- Assignee set to fixeria

- Priority changed from Normal to High

- % Done changed from 0 to 90

Hi Keith,

thanks for this report!

I've managed to reproduce the problem in my virtual network,
and implemented a fix for that, please see:

https://gerrit.osmocom.org/11341/

In short, the problem is that 'structured' SS requests are not answered at all.
We should reject such requests by sending returnError message until we start to support them.

#3 - 10/13/2018 09:38 AM - keith

Nice! Thanks for fixing that!

I wonder if there should be some kind of "failsafe" timer also on the MSC (or maybe it's BSC side) that would shutdown the channel in the case that the HLR became unresponsive.

I should have also included a trace of the call that I mentioned in the email.. Let me try to get that now before I pull your HLR patch....

#4 - 10/13/2018 10:12 AM - keith

- File abis.pcap added

OK, Maybe I'll make a new ticket for this, but as it is possibly not easy to reproduce without the bug mentioned here, I'll put it here for now..

This is what I do and what I observe, using a Nokia 6070.

```
Dial *#21# + SEND
```

Phone says **Requesting..** and I observe SDCCH activity on the spectrum Uplink.
I press END on the phone.
Phone says **Request not Confirmed**, appears to go to standby and SDCCH Uplink actvity continues.
I call a number on phone and press SEND
Phone immediately says "Error in connection" and I observe TCH activity on spectrum.
Phone appears to returns to standby and TCH continues.

BSC at this point shows:

```
OsmoBSC# show lchan s
BTS 0, TRX 0, Timeslot 1 TCH/F, Lchan 0, Type TCH_F, State ESTABLISHED - L1 MS Power: 5 dBm RXL-FULL-dl:  -47 dBm RXL-FULL-ul:  -50 dBm
```

Some several minutes later, phone TX is still active, TCH is still active.
I issue drop bts from BSC
Phone display shows **Request not completed**

(in the pcap, I didn't wait so long before dropping the bts)

#5 - 10/13/2018 10:21 AM - keith

- File local.pcap added

#6 - 10/13/2018 10:22 AM - keith

Adding Capture of A/GSUP for above description.

#7 - 10/13/2018 10:44 AM - keith

- File abis.pcap added

Further,

With the HLR patch in place, the KRZR now camps, issues the SS and goes idle. All Good. :)
Subsequently calling the KRZR from the Nokia (with the error provoked in freeswitch by #3650) results in a lingering SDCCH on the KRZR!

(with osmo-sip-connector patched to override the payload_type, call sets up, connects, and completes with success)

Still, It strikes me we are missing something. abis pcap of the above attached.

#8 - 10/13/2018 10:53 AM - keith

- File local.pcap added

A / GSUP pcap for above. (there's some OsmoVTY, SIP and freeswitch console noise in there too)

Note, these A /GSUP captures were not captured at the same time as the abis, but it was the same sequence of events.

#9 - 10/15/2018 07:25 PM - fixeria

- Related to Feature #3655: Introduce self-destruction timer for SS/USSD connections added

#10 - 10/15/2018 07:34 PM - fixeria

Hi Keith,

> I wonder if there should be some kind of "failsafe" timer
> also on the MSC (or maybe it's BSC side) that would shutdown
> the channel in the case that the HLR became unresponsive.

Yep, definitely. I created an issue, please see: #3655.

> With the HLR patch in place, the KRZR now camps,
> issues the SS and goes idle. All Good. :)

Should we mark this issue as "resolved" then?

> Subsequently calling the KRZR from the Nokia
> results in a lingering SDCCH on the KRZR!

If it's still related to the SS/USSD, I am feeling a bit lost :)

#11 - 11/27/2018 11:06 PM - fixeria

- Status changed from Feedback to Resolved

- % Done changed from 90 to 100

The following test case confirms that the problem was actually solved:

https://gerrit.osmocom.org/#/c/osmo-ttcn3-hacks/+/11960/

so, closing.

Files

local.pcap	10.1 KB	10/12/2018	keith
SS-abis.pcap	34.8 KB	10/12/2018	keith
USSD-good-abis.pcap	4.14 KB	10/12/2018	keith
abis.pcap	124 KB	10/13/2018	keith
local.pcap	109 KB	10/13/2018	keith
abis.pcap	28.2 KB	10/13/2018	keith
local.pcap	178 KB	10/13/2018	keith