osmo-remsim - Bug #4409

osmo-remsim-client-st2 (or firmware?) gets stuck on PTS

02/20/2020 09:02 PM - laforge

Status:	Stalled	**Start date:**	02/20/2020
Priority:	Low	**Due date:**	
Assignee:	Hoernchen	**% Done:**	80%
Category:	remsim-client		
Target version:			
Spec Reference:			

Description

In the test setup at my home office, I can occasionally see osmo-remsim-client-st2 get stuck when the Modem (in this case a Quectel EC20) is performing PTS with the card.

In the log of osmo-remsim-client-st2 I can see:

```
SIMtrace => PTS req: ff 10 94 7b 00 00 ^M
SIMtrace -> 01 07 00 00 00 00 15 00 04 ff 10 94 7b 00 00 ff 10 94 7b ^M
SIMtrace => PTS req: ff 10 94 7b 00 00 ^M
SIMtrace IRQ 01 04 00 00 00 00 15 00 13 00 00 00 00 00 09 04 0a 80 25 00 00 ^M
```

after which the communication doens't proceed. After a long time, the modem seems to retry without PTS and then proceeds with normal SIM card communication.

The SIM Card ATR in this case is 3b7d9400005555530a7486930b247c4d5468.

History

#1 - 02/20/2020 09:09 PM - laforge

- Subject changed from osmo-remsim-client-st2 (or firmware?) gets stuc on PTS to osmo-remsim-client-st2 (or firmware?) gets stuck on PTS

- Category set to remsim-client

Observed with remsim-client 0.2.2.46.3598

#2 - 02/21/2020 08:05 PM - laforge

Serial Console output at the time this happens:

```
-I- 0: ATR set: 3b 7d 94 00 00 55 55 53 0a 74 86 93 0b 24 7c 4d 54 68
-I- 0: De-asserting modem reset
-I- 0: RST released
-I- 0: RST asserted
-I- 0: VCC activated
-I- 0: CLK activated
-I- 0: RST released
-I- 0: computed Fi(1) Di(1) ratio: 372
-I- 0: computed Fi(9) Di(4) ratio: 64
-I- 0: send_tpdu_header: 00 a4 00 04 02
-I- 0: flush_rx_buffer (5)
```

So based on this we can see that the firmware **thinks** it has sent the heaer of the first APDU after the PTS, but somehow the simtrace2 host software doesn't claim to know anything about it.

#3 - 02/21/2020 08:37 PM - laforge

- % Done changed from 0 to 20

Doing a usbmon/tshark capture shows the following message on the USB BULK IN endpoint:

```
0106000000001300010000000050000a4000402
```

This clearly contains the APDU header of the first APDU after the PTS. so it appears to be the remsim-client software that's somehow loosing/dropping it.

#4 - 02/21/2020 08:41 PM - laforge

- File 20200221-qmod-pts.pcapng added

#5 - 02/21/2020 09:00 PM - laforge

problem can be avoided by the following patch:

```
diff --git a/src/client/simtrace2-remsim_client.c b/src/client/simtrace2-remsim_client.c
index 2929574..08f37ea 100644
--- a/src/client/simtrace2-remsim_client.c
+++ b/src/client/simtrace2-remsim_client.c
@@ -1164,6 +1164,9 @@ static void main_body(struct cardem_inst *ci, struct client_config *cfg)

        allocate_and_submit_irq(ci);
        allocate_and_submit_in(ci);
+       allocate_and_submit_in(ci);
+       allocate_and_submit_in(ci);
+       allocate_and_submit_in(ci);

        while (!g_leave_main) {
                osmo_select_main(false);
```

This ensures multiple URB are submitted and we're never starving the device of IN EP URBs.

#6 - 02/21/2020 09:12 PM - laforge

- % Done changed from 20 to 80

Patch submitted in https://gerrit.osmocom.org/c/osmo-remsim/+/17243

#7 - 02/22/2020 09:41 PM - laforge

I'm again observing this despite the four submitted URBs :(

#8 - 03/04/2020 09:15 PM - laforge

As an interim work-around we can of course simply advertise an ATR that supports only lower speeds.. but I don't really like that and would prefer a proper solution.

#9 - 06/13/2020 06:04 PM - laforge

- Status changed from In Progress to Stalled

#10 - 02/06/2021 08:55 AM - laforge

- Assignee changed from laforge to Hoernchen

- Priority changed from High to Low

Files

20200221-qmod-pts.pcapng	4.32 KB	02/21/2020	laforge