SIMtrace - Bug #2614

simtrace_hdr randomly appears in APDU payload

11/03/2017 04:58 AM - lukash

Status:	New	**Start date:**	11/03/2017
Priority:	Normal	**Due date:**	
Assignee:	lukash	**% Done:**	0%
Category:	SIMtrace firmware		
Target version:			
Spec Reference:			

Description

A "random" sequence of bytes (which seems to look like simtrace_hdr) appears in APDU payload from time to time, breaking the apdu_split mechanism.

```
USB MSG: sh->cmd: 1, sh->flags: 0, sh->res[9, 5], payload: 00 a4 00 04 02 a4 6f 07 61 2a 00 c0 00
00 2a c0 62 28 82 02 41 21 83 02 6f 07 a5 0f 80 01 71 c0 01 00 91 04 7f 20 6f 07 92 01 00 8a 01 05
 8b 03 6f 06 03 80 02 00 09 88 01 38 90 00 01 00 09 05 00 b0 00 00 09 b0 08 29 03 30 10 66 03 91 1
2 90 00
APDU: 00 a4 00 04 02 6f 07 61 2a
APDU: 00 c0 00 00 2a 62 28 82 02 41 21 83 02 6f 07 a5 0f 80 01 71 c0 01 00 91 04 7f 20 6f 07 92 01
 00 8a 01 05 8b 03 6f 06 03 80 02 00 09 88 01 38 90 00
APDU: **01 00 09 05** 00 b0 00
APDU: 00 09 b0 08 29 03 30
APDU: 10 66 03 91 12 90 00
```

The 01 00 09 05 seems to be sh->cmd, sh->flags, sh->res (2 bytes)
Guessing this is because somehow simtrace_hdr is appended into the data or 2 separate messages are somehow concatenated into one.

This seems to have been introduced after v0.5 firmware (IMHO it is in firmware).

History

#1 - 11/03/2017 07:50 AM - lukash

Got a little further - seems like two separate messages sent by the firmware arrive into (what appears to be) a single message (as seen by host software).

Anybody has an idea what might be causing such behavior?

Trace from firmware (SIM_HEAD debug is in send_rctx() in iso7816_uart.c right before the memcpy of header into rxtc->data):

```
[000054] USBT(D=00202BE0, L=0023, P=00) H8/T4: 01 00 09 05 B0 00 00 0C / FF FF 90 00
[000055] SIM_HEAD(D=00202FA0, L=0040)

[000056] USBT(D=00202FA0, L=0040, P=00) H8/T4: 01 00 09 05 80 10 00 00 / 00 00 00 08
[000057] SIM_HEAD(D=00203360, L=0064)

// the following are two separate messages with two separate simtrace_hdr headers but they arrive as one to th
e host SW
[000058] USBT(D=00203360, L=0064, P=00) H8/T4: 01 00 09 05 91 2A 80 12 / 02 A4 2F 00
[000059] SIM_HEAD(D=00203720, L=0053)

[00005A] USBT(D=00203720, L=0053, P=00) H8/T4: 01 00 09 05 61 27 00 C0 / 01 F0 90 00
[00005B] SIM_HEAD(D=00203AE0, L=0045)

[00005C] USBT(D=00203AE0, L=0045, P=00) H8/T4: 01 00 09 05 00 B2 01 04 / FF FF 90 00
[00005D] SIM_HEAD(D=00203EA0, L=0045)
```

Trace from host SW:

```
URB: 01 00 09 05 b0 00 00 0c b0 63 73 ff ff ff ff ff ff ff ff ff ff 90 00
APDU: 00 b0 00 00 0c 63 73 ff ff ff ff ff ff ff ff ff ff 90 00
```

```
URB: 01 00 09 05 80 10 00 00 1e 10 ff ff ff ff 7f 9d 00 df bf 00 00 1f e2 00 00 00 c3 f0 00 07 00 01 60 00 51
00 00 00 00 08

                                                                                |> second message start
s right here, this header is therefore considered part of the APDU stream
URB: 01 00 09 05 91 2a 80 12 00 00 2a 12 d0 28 81 03 01 25 00 82 02 81 82 05 08 56 6f 64 61 66 6f 6e 65 8f 08
01 4d 2d 42 61 6e 6b 61 8f 09 02 4d 2d 50 6c 61 74 62 79 90 00 00 a4 00 04 02 a4 2f 00 01 00 09 05 61 27 00 c0
 00 00 27 c0 62 25 82 05 42 21 00 21 02 83 02 2f 00 a5 09 80 01 71 c0 01 00 92 01 00 8a 01 05 8b 03 2f 06 03 8
0 02 00 42 88 01 f0 90 00
APDU: 80 10 00 00 1e ff ff ff ff 7f 9d 00 df bf 00 00 1f e2 00 00 00 c3 f0 00 07 00 01 60 00 51 00 00 00 00 08
 91 2a
APDU: 80 12 00 00 2a d0 28 81 03 01 25 00 82 02 81 82 05 08 56 6f 64 61 66 6f 6e 65 8f 08 01 4d 2d 42 61 6e 6b
 61 8f 09 02 4d 2d 50 6c 61 74 62 79 90 00
APDU: 00 a4 00 04 02 2f 00 01 00 <- first 2 bytes of the header (01 00)
APDU: 09 05 61 27 00 c0 00 <- second 2 bytes of the header (09 05)
APDU: 00 27 c0 62 25 82 05
APDU: 42 21 00 21 02 83 02

URB: 01 00 09 05 00 b2 01 04 21 b2 61 1b 4f 10 a0 00 00 00 87 10 02 f4 20 f0 01 89 00 00 01 ff 50 07 56 46 20
55 53 49 4d ff ff ff ff 90 00
```

#2 - 11/03/2017 08:54 AM - lukash

This is a result of an older non-merged code by Min Xu: https://lists.osmocom.org/pipermail/simtrace/2014-January/000621.html

Needs to be merged in in a way that won't break openocd build as Harald mentioned here:
https://lists.osmocom.org/pipermail/simtrace/2014-November/000003.html

I will follow up on this and will try to get that done - it seems to be an essential part to the Min Xu set of patches to be complete.