t=0x87494a0
cell=0x874dd28 [0,0]

Contents: [Dobrica PavlinuÅ¡iÄ 's random unstructured stuff]

voice info

```
17:42 < dpavlin> stupid question about by first experiment with osmocom-bb
http://blog.rot13.org/2011/01/osmocom-bb_-_free_software_finally_comes_to_gsm.html - are hex
                 numbers I see scroll by voice data by any chance or controll stream?
17:42 < steve|m> dpavlin: that's the voice_ind
17:43 < steve|m> http://bb.osmocom.org/trac/changeset/a4e34316c403a49ca57fd907e55a16b721629e35/sr
17:43 < steve|m> so maybe revert this commit in your local branch if you don't need that
                 (transferring voice data to the host)
17:45 < dpavlin> Great. With something like pipe I could go a long way :-)
17:46 < dpavlin> Can I inject it over serial port? For something like text2speech?
17:46 < steve|m> tnt has code for that, but he hasn't committed it yet
17:46 < steve|m> jolly even has written an interface to LCR
17:49 < dpavlin> I would love to help test it, if such help is needed.
```

- http://bb.osmocom.org/trac/changeset/999254a3a6641ea112b48c1eca65599fb9989185
- GSM 06.10 encoder/decoder http://www.quut.com/gsm/

```
19:21 < dpavlin> tnt: do you have any pointers to information about calypso voice format I can re
19:23 < dw> the code? :)
19:26 < dpavlin> I tried reading code under src/target/firmware/calypso but I'm probably looking
                 because I'm not closer to understanding voice.raw format than I was few days ago
19:30 < steve|m> dpavlin: looked at
http://bb.osmocom.org/trac/browser/src/target_dsp/calypso/dsp_sniff.S?rev=d1cb8ea9b784c7acbafbb2f
19:31 < tnt> steve|m: that's not for voice.raw
19:31 < tnt> There is just no written reference anywhere of the buffer format.
19:31 < steve|m> ah, sorry, confused that..
19:44 < tnt> dpavlin: from memory, it's all the class 1 bits, then some bits always at 0 (4 bits
             class 2 bits of a GSM 610 frame.  They're packet in 16 bits works, MSB first
```

```
1297284215 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> I have a question about burst_ind branch
@1297284218 <mkf00!~mkf00@85-127-108-141.dynamic.xdsl-line.inode.at> hallo
@1297284279 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> In l1ctl_burst_ind I understand that the
@1297284286 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> is this correct?
@1297284318 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> this is because I think that both must b
@1297284347 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> tnt?
@1297284376 <tnt!~tnt@mojito.smartwebsearching.be> no it's not correct
@1297284389 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> uhm!
@1297284391 <tnt!~tnt@mojito.smartwebsearching.be> the two stealing bits are at the end, the DSP
@1297284439 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> both are together?
@1297284440 <tnt!~tnt@mojito.smartwebsearching.be> On the air you are correct they're in the midd
@1297284538 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> from my code:
@1297284542 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> <0001> layer3.c:418 LEO BURST: 58 93 b5
```

```
@1297284605 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> we don't need the first 4 bits
@1297284618 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> but the next one is 1
@1297284633 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> only one stealing bit filled?
@1297284671 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> only one stealing bit with 1?
@1297284908 <tnt!~tnt@mojito.smartwebsearching.be> Fatuo: yup. so ?
@1297284945 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> I thought that both must be the same....
@1297284983 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> Can be FACCH and voice/data in the same
@1297285078 <tnt!~tnt@mojito.smartwebsearching.be> well, you think wrong :)
@1297285108 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> oh
@1297285111 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> tanks :)
@1297285111 <tnt!~tnt@mojito.smartwebsearching.be> you need to re-read GSM 05.03. TCH has diagona
@1297285148 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> ok, i will do right now, thanks a lot
@1297285149 <tnt!~tnt@mojito.smartwebsearching.be> so the 4 * 114 bits are split into 8 half burs
@1297285247 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> I see
@1297285275 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> I'll go re-reading that doc
@1297285277 <Fatuo!~n0p@79.198.19.95.dynamic.jazztel.es> bye
```

- http://git.osmocom.org/gitweb?p=gapk.git;a=summary

A5/1

- http://reflextor.com/trac/a51/browser/tinkering
- http://opensource.srlabs.de/projects/a51-decrypt/files

```
git clone git://git.srlabs.de/kraken
```

- http://srlabs.de/research/decrypting_gsm/
- http://srlabs.de/uncategorized/airprobe-how-to/

```
13:35 < tomash2> [Thu 13:56] Hi
13:35 < tomash2> [Thu 13:58] When receiving bursts via sylvain/burst_ind, is the frame number for
13:35 < tomash2> [Thu 13:59] Assembled packets appear to be on differrent channel that uplink one
13:35 < tomash2> [Thu 14:01] It works to do fn=fn-15 for unencrypted packets, but not for encrypt
13:35 < tomash2> [Thu 14:01] So how to get correct fn for uplink bursts?
13:35 < tnt> [Thu 14:06] the fn is correct, your code is wrong obviously ...
13:35 < tomash2> [Thu 14:08] Strange, downlink decrypting works, and I do uplink the same way...
13:35 < tomash2> [Thu 14:08] Thakns, I'll go to search for the bug...
13:35 < tnt> [Thu 14:10] ... then that's your problem.
13:35 < tnt> [Thu 14:10] uplink is _not_ same as downlink
13:35 < tnt> [Thu 14:10] the first 116 bits of A5 is for DL, then you need the 116 after that for
13:35 < tomash2> [17:11] tnt: And these second 116 bits are computed from Kc and fn the same way
13:35 < tnt> [17:13] yup
13:35 < tnt> [17:13] 114 not 116 btw
13:35 < tnt> [17:13] stealing bits aren't ciphered
13:35 < tnt> [17:13] (afair)
13:35 < tomash2> [17:14] tnt: That's what I'm doing. But it is not working for uplink
13:35 < tnt> [17:15] well you're doing it wrong :)
13:35 < tomash2> [17:16] tnt: maybe :-)
13:35 < tnt> [17:16] your a5 keystream genreator should generate 228 bits of outpout per frame, t
13:35 < tomash2> [17:17] tnt: huh
13:35 < tnt> [17:17] That's what I told you above:
13:35 < tnt> [17:17] 14:10 < tnt> the first 116 bits of A5 is for DL, then you need the 116 after
13:35 < tomash2> [17:17] so uplink bits are _not_ computed from fn of the uplink burst?
13:35 < tnt> [17:18] ... of course they are
13:35 < xorAxAx> [17:18] frame count!
13:35 < tnt> [17:19] xorAxAx: frame count is just another representation of fn ... (how to feed t
13:35 < xorAxAx> [17:19] yeah
13:35 < tnt> [17:20] tomash2: for SDCCH the UL and DL are in different frame, so you would only u
```

```
13:35 < tnt> [17:21] but it doesn't matter ... UL is always the second and you _have_ to compute
13:35 < tomash2> [17:22] tnt: I'm talking about SDCCH all the time, I didn't try TCH yet...
13:35 < tnt> [17:22] and as I said : It doesn't matter ...
13:35 <Bassam> Hi.
13:35 <Bassam> What is the relation between the frame numbers in both the UL and DL stages in the
```

Neo

- http://www.steve-m.de/projects/osmocom/0001-for-testing-add-TX-support-for-gta0x-devices.patch

BTS

- http://www.246tnt.com/gsm/rx_filter.html