OsmoMSC - Bug #2872

OsmoMSC doesn't check if CIPHER MODE COMPLETE contains cipher that matches REQUEST

01/24/2018 09:37 PM - laforge

Status:	In Progress	**Start date:**	01/24/2018
Priority:	Normal	**Due date:**	
Assignee:	stsp	**% Done:**	0%
Category:	A interface (general)		
Target version:			
Resolution:			

Description

When the MSC requests a cipher from a set of ciphers as stated in the BSSMAP CIPHER MODE REQUEST, we should check if the (bsc-)chosen cipher actually is within that set.

Care must be taken as the 'chosen algorithm' IE is optional.

A corresponding TTCN-3 test case should be developed, trying to COMPLETE with a cipher that's not in the set of those REQUESTed

History

#1 - 05/17/2018 01:58 PM - laforge

- Assignee changed from sysmocom to stsp

#2 - 12/17/2018 12:36 PM - stsp

"BSSMAP CIPHER MODE REQUEST" doesn't seem to exist.
You probably meant BSSMAP CIPHER MODE CMD instead?

#3 - 12/17/2018 12:36 PM - stsp

- Status changed from New to In Progress

#4 - 12/17/2018 02:12 PM - stsp

This proposed patch adds a TTCN3 test for this issue:
https://gerrit.osmocom.org/#/c/osmo-ttcn3-hacks/+/12332

At present the MSC responds with a LU reject after receiving a CIPHER MODE COMPLETE with an invalid cipher.
The test looks for this LU reject and passes when it is received.

Is this the correct behaviour? Should the MSC respond in some other way?

#5 - 12/17/2018 02:59 PM - neels

re "command" vs "request": the things can be named differently on the layers, e.g. there's the Cipher Mode Command on BSSMAP, but Cipher Mode Request on 04.08...

#6 - 12/18/2018 11:02 AM - stsp

The above test has been merged. neels says the current osmo-msc behaviour which the test checks for (expect a LU reject) is correct as it is.
Can this issue be closed?

#7 - 12/18/2018 12:44 PM - neels

this issue says that osmo-msc should check that the cipher matches the request,
and the issue implies that osmo-msc doesn't check that.
If it turns out that osmo-msc does indeed reject a mismatch already, that's nice.

How about the side thing there, if the chosen algorithm is not provided in the response?
I guess osmo-msc should accept then. Does it? (If they mismatch then, the ciphered data will not be decipherable anyway.)
Maybe duplicate the test for that situation.

#8 - 12/18/2018 04:32 PM - stsp

See https://gerrit.osmocom.org/c/osmo-ttcn3-hacks/+/12347 for additional tests,
and https://gerrit.osmocom.org/c/osmo-msc/+/12349 for related osmo-msc changes.

The tests are not complete yet -- they pass both with and without the osmo-msc changes
because they don't verify which cipher the MSC really ends up using. Could you suggest
a good way of doing that?