3GPP TSG SA WG3 Security — S3#35 **S3-040802**

St Paul's Bay, Malta, October 5-8, 2004

Source:	**Siemens**
Title:	**SMS Fraud countermeasure**
Document for:	**Discussion and Decision**
Agenda Item:	**6.2**

1 Introduction

This contribution provides a follow-up of the discussion on ‘SMS fraud countermeasures’. It collects and analyses the received responses from CN4 and T2. Also the security and implementation variants of the TCAP handshake mechanism are analyzed.

2 Analyzing the responses from CN4 and T2.

As described by [T2-040329] the use of the TCAP handshake for MAP mt-forward-SM messages will lead to increased MAP traffic on the SS7-network. This may lead in a worst case heavy load scenario to degradation of SMS delivery when SS7 resources are not adequately provisioned for the increased amount of SS7-traffic due to SMS. The fear for SMS delivery degradation may be originating from the assumption that the TCAP handshake shall be used for all MAP mt-forward-SM messages of all terminating operators. This contribution however proposes this to be an optional mechanism to use. This optional use will however come at the expense of additional MSC/SGSN administration as will be described in section 3.

A first LS from CN4 [N4-041193] did take a deeper look at the TCAP handshake solution for mt-forward-SM messages. It is reported back that the mechanism is already implemented in application context versions 2 and 3 (but can not be used with version 1) for Short Message Transfer for cases where the length of the SM payload exceeds a certain limit, and it can easily be extended to be applied also for Short Messages with a shorter payload. Also CN4 acknowledged that the handshake mechanism doubles the signalling load on the interfaces between SMSC (SMS-GMSC) and MSC / SGSN for MT short message transfer. **CN4 discussions were inconclusive with respect to mandating this for implementation or making the mechanism optional**. The TCAP handshake can be mandated for implementation from Rel-6 on for mt-Forward-SM (*which then requires that either application context 2 or 3 shall be supported*), while still being optional for use and as such leaving the decision up to the operator. An operator (*note that in the typical fraud scenario more then one operators (SS7) network is involved*) who would not like to take the disadvantages can still decide (in agreement not to use it).

A second LS from CN4 [N4-041204] highlights that CN4 has discussed ‘*whether a solution addressing only the particular SMS fraud scenarios of ‘faking’ and ‘spoofing’ is desired, or whether in fact a greater remit is to be addressed. That remit could be to secure the SS7 network as a whole, whilst also providing a solution to the immediate SMS fraud issues*.’ Two GSMA subgroups (i.e. IREG and SG) have been asked to provide some guidance on the timing issues for the long term solution while no feedback was given by CN4 on desired scope of a solution. It is believed that the TCAP handshake based solution is a **shorter-term applicable solution**[1] that could be used as a means to detect SMS-spoofing, while any long-term solution will take much longer time to be ready for use. **At the moment the long-term solution becomes available, the use of the short-term solution can be stopped**. This is an operator’s business decision with no impacts

[1] A pre-requisite for the short-term solution to succeed is that as few as possible additional requirements are put on the terminating MSC/SGSN.

on standardization. It is 3GPP's responsibility to provide the operators the tools for detection of SMS-fraud. It is however up to the operator's to use this tool, knowing the advantages and disadvantages. An operator may require suspicious SMSC-partners to upgrade to application context 2/3 for mt-forward-SM, making the TCAP handshake available for use (whenever required) in order to be able to trace back the fraud.

The next section looks at different variants of realization after having looked at some raised security issues of the TCAP handshake solution.

3 Different solution variants

3.1 Security analysis

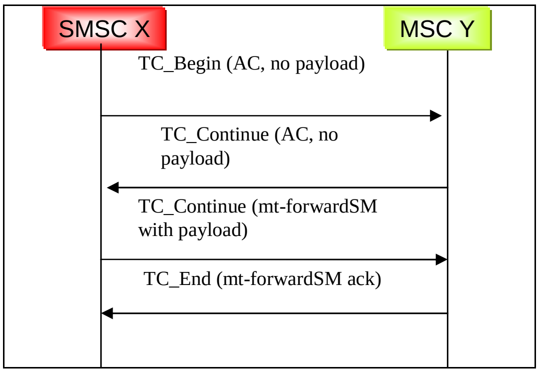
SMSC X
MSC Y
TC_Begin (AC, no payload)
TC_Continue (AC, no payload)
TC_Continue (mt-forwardSM with payload)
TC_End (mt-forwardSM ack)

Figure 1: MAP Forward SM messages solution for long payload lengths

Within [S3-040581] the use of the TCAP handshake was described. This reads (summarized): "*If the MSC receives an mt-forward-SM MAP messages which use the TC_Continue to transfer the MAP payload then it is guaranteed that the SS7 calling party address of the (empty) TC_Begin message is authentic, otherwise the first TC-continue message would be sent to the falsified address and dropped there. The correct message flow is guaranteed by the TCAP transaction capabilities (use of Transaction ID). Matching parts of this SS7 calling party address (country code (CC), national destination code (NDC)) with the SMSC address received in the MAP message, implicitly verifies CC and NCC of the SMSC address.*"

There are some ways in which a fraudulent SMSC (G-MSC) may try to circumvent the implicit SS7 address authentication provided by the TCAP handshake.

A) A first easy to use (but also to detect) possibility is to include a falsified SMSC address within the TC_Continue (mt-forwardSM with payload). This can be detected by the receiving MSC by checking if the received SMSC address (in the third message) matches with the SS7-address the message is received from, and consequently the transaction can be rejected in real-time. **This requires that the MSC implements a table of allowed addresses including a list of SMSC-addresses and the allowed SS7 addresses may be sent from (table 1). This must match with the SS7-address of the first TCAP-message.** Alternatively if such a table would not be used then all addresses can be logged and analyzed afterwards**. Such a table could also be beneficially used to reject SMS traffic from a malicious party that predicted the TCAP-ID in the third message but sent it from a wrong SS7-address.**

B) As the implicit authentication also relies on the use and match of the TCAP transaction identifiers, the fraudulent SMS sender (who wants to be anonymous and fakes the addresses) may try to predict the transaction identifier which will be used within the second TCAP message. If the SMS sender can predict the transaction ID then he will be able to send successfully a third message, without having received the second message. For this purpose the fraudulent sender will need to analyze the

TCAP Transaction ID [2]assignment at the MSC to calculate the highest probable guess[3]. Please note that the fraudulent sender is not able to reset the TCAP transaction ID of the MSC. The receiving MSC obtains now (a lot of) unsuccessful SS7 traffic for SMS transfer, being an indication of fraudulent injection, but the MSC is not able to pinpoint the sender at once. The amount of SS7 traffic to get the fraudulent messages through has increased such that that the Senders SS7-address may be more easily locatable. **The cost for the fraudulent SMSC to get the messages through will increase inverse with the probability of a successful transaction ID guess**. This comes on top of the additional (non standard implementation) ability of the senders SMSC (or G-MSC) to generate such messages. It is assumed that many TCAP implementations assign the Transaction Identifiers in a predictable implementation specific way. The countermeasures to this predictability could be similarly as used in making the TCP sequence number more unpredictable. A first measure is to require a certain number of increments of the Transaction ID per second. A more sophisticated measure is to randomize the increments through the use of a cryptographic algorithm. The history on unpredictable[4] TCP sequence number generation has learned that satisfying the 'unpredictability'-requirement is not so easy to fulfill. In the typical fraud scenario the SMSC (G-MSC) is far away from the MSC, such that the probability to guess the right TCAP number is more difficult then in a neighborhood configuration. *To have a short term ready solution the impacts on existing TCAP numbers implementations shall be minimized.* **If SA3 thinks that cryptographically based TCAP-ID would be required then it is proposed to further study the effects as the TCAP ID might be used for other features (e.g. optimized SS7 link selection).**

3.2 Solution variants

The basic assumption here is that the use of the TCAP handshake for mt-Forward-SM cannot be mandated i.e. it remains optional for use. The operators wanting to use the feature need to agree with the roaming partners to upgrade the equipment to application context2 or 3 for mt-Forward-SM.

Define an 'operator group-1' as a trusted operator group and 'operator group-2' as an un-trusted operator group.

Option 1: Agree group-1 to use the TCAP handshake, while group-2 would use no TCAP handshake.

The rationale is that the trusted partners would probably have no problem with using the TCAP handshake. With the goal to move more and more operators into the trusted group, this would lead in the end that all mt-Forward-SM traffic (that terminates at a certain operator), will be secured using the TCAP handshake.

Option 2: Agree group-2 to use the TCAP handshake, while group-1 would use no TCAP handshake.

The goal would be here to limit the extra load on the SS7-network. With the goal to move more and more operators into the trusted group[5], this would lead in the end that no traffic (that terminates at a certain operator), will be secured using the TCAP handshake. If every MSC and SMSC (G-MSC) is required to implemented the TCAP handshake, in case of new originating fraud, the TCAP handshake could be switched on. This is a disadvantage. Moreover without additional measures the group-2 members will try to act as a group-1 member so address checking seems to be required.

In the assumption that only a few other operators can use the TCAP handshake (which is currently the case), then Option 1 approach would be the best. From a practical point of view the larger and more reliable

[2] The originating and receiving TCAP ID have a length of 32-bit.

[3] The TCAP transaction ID prediction has similarities with TCP sequence number prediction

[4] More info on how TCP implementation failed to provide 'random' TCP sequence number generation can be found in http://lcamtuf.coredump.cx/newtcp/.

[5] This is now pure trust, which is not enforced by the use of the TCAP mechanism

(=trusted) operators are more likely to quickly switch to handshake (option 1). Trust who can run the TCAP handshake, and supervise the SMS transfer for the group-2 more closely (possibly limiting the SMS transfer capabilities). *Option 1 is preferred as it allows a gradual use over time of the TCAP handshake for those operators wishing to use it.*

Independent from the above options this requires that the MSC can make a secure decision whether the received mt-forward-SM requires a TCAP handshake or not. This requires that the MSC shall implement a policy table of originating SS7-addresses for which a TCAP handshake is (not) required. A fraudulent SMSC would try to use an SS7-address which does not require the TCAP handshake, so careful administration is necessary and even the content of the MT-forward-SM message without TCAP handshake should be screened in similarity with table 1 mentioned in the section 3.1. The needed tables require a lot of administration, but fortunately the required tables seem to be static in nature, so the difficulty lies in the initial set up.

4 Conclusions

It is proposed to

1) Document the TCAP handshake short term solution for MT-forward-SM authentication, and the solution option 1 within an informative Annex to TS 33.200.

2) To carefully consider any additional impacts as this will delay the realization and acceptance of a solution. Therefore it is proposed not to require any change to the TCAP generation mechanisms. Additional tables with SS7/SMSC address seems to be required but cannot provide an absolute guarantee.

5 References

[S3-040581]: SA3#34: SMS Fraud countermeasure (Siemens, Vodafone).

[T2-040329]: LS from T2 on ‘SMS Fraud countermeasures’.

[N4-041204]: LS from CN4 on ‘Evaluation of the alternatives for SMS fraud countermeasures’.

[N4-041193]: LS from CN4 on ‘SMS Fraud countermeasures’.