3GPP TSG SA WG3 Security — S3#34 **S3-040581**

July 6 - 9, 2004 **comments to S3-040550**

Acapulco, Mexico

Source: **Siemens, Vodafone**

Title: **SMS Fraud countermeasure**

Document for: **Discussion and Decision**

Agenda Item: **7.2**

1 Introduction

At last SA-plenary (SA#24), contribution [SP-040279] was presented which asked SA3 to complete the work on MAPsec. While admitting that MAPsec is a general building block and can be used for combat the SMS fraud, it needs also be said that this building block is not ready to be deployed. Furthermore, an homogenous use in all networks is required. From a standardization point of view the necessary SA3 effort to standardize an SMS-MAP profile is very low, while the work on the Ze-interface (between the KAC and the MAP nodes) will still need some time to complete. The introduction of the MAPsec protocol (only the Zf-interface) within the networks will require some years. But yet the GSMA [S3-040492] seems to require a solution that could be deployed much earlier in the field. It can be expected that the use of non 3GPP countermeasures (such as the use of screening boxes) will only increase over time such that at the time of MAPsec deployment, the business case for MAPsec use may be worse than expected today. This contribution proposes a solution specifically for SMS fraud that could be deployed within a much shorter timeframe than MAPsec. Furthermore the proposed solution seems to require minimal standardization/implementation efforts.

2 SMS fraud scenario(s).

As described by [SP-040279] the typical fraud scenario consists in sending many[1] MAP *Forward Short Messages* (mt-forwardSM) with the source SMSC address spoofed. The recipient MSC acknowledges the message delivery to the SMSC, and in addition charging information is produced which, among other relevant information, captures the SMSC address from which the short message was received. The consequence is a misalignment of the accounting mechanism between the originating network and the terminating network. The terminating network (which has terminated the SMS traffic) will request more money from the "originating" network than justified. So beside the fraudulent SMS content this scenario results in wrong interoperator accounting.

Figure 1 describes this scenario.

[1] The fraudulent SMSC uses an own database of collected triples { MSISDN/IMSI/MSC }. The fraudulent SMSC database need not be accurate as charging is avoided by faking the adresses.

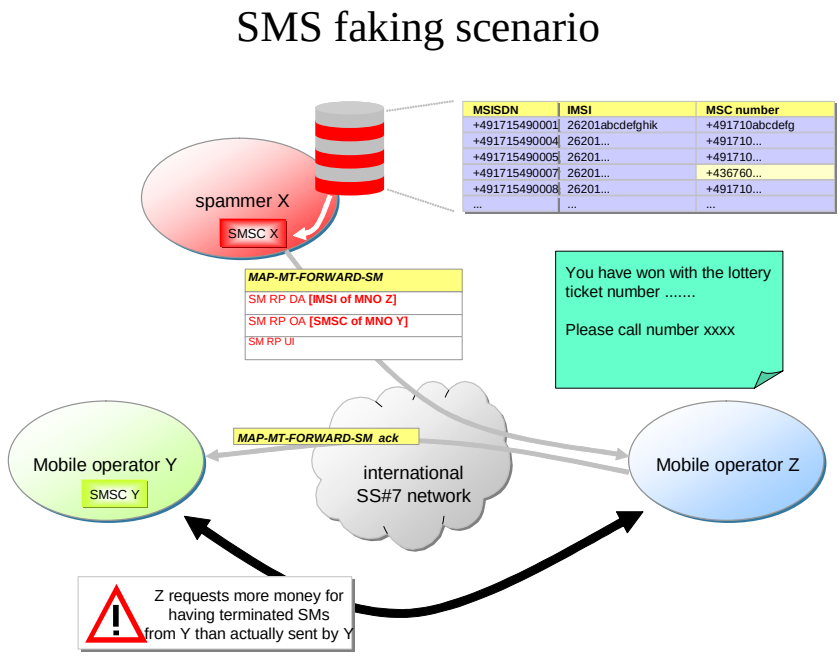

Figure 1: SMS fraud scenario

3 A proposed countermeasure

The fact that the SMSC address contained in the mt-forwardSM message is spoofed can be detected by introducing a TCAP-handshake between the MSC that receives the MAP mt-forwardSM message and sender of the message. **The TCAP handshake implicitly guarantees that the SS7-adress of the mt-ForwardSM message sender was ok, and therefore this SS7 address can be used to check the validity of the received upper layer address before sending the ack message.**

Nothing new has to be standardized for this, as the actual concept is available for use already. 3GPP defines the exchange of MAP dialogue portions without containing MAP operations (component portions) at the beginning of a MAP dialogue. This exchange is commonly used in the MAP signaling for SMS.

Example (SMS MT, mt-forwardSM):

When the SMS payload (sm-RP-UI) does not exceed a certain size, the transfer of the MAP mt-forward-SM message (See Figure 2) can be accommodated within one TC-Begin (MAP Version2). However when the size of the payload is above this limit, it might not fit in a MAP V2 message that contains a MAP Dialogue Portion (as the TC-Begin does). However, there is a mechanism available to transfer the longer SMS-payload within a MAP V2 dialogue using the message exchange mentioned above (see Figure 3).

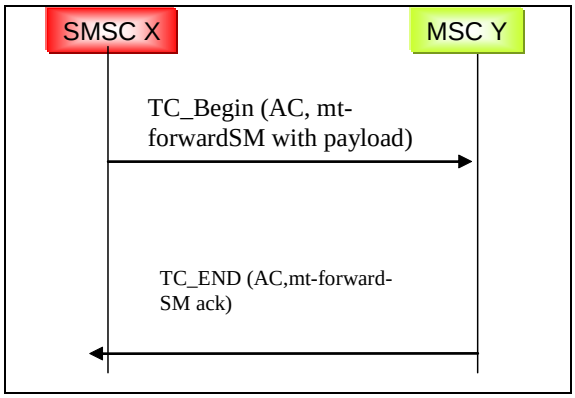

Figure 2: MAP Forward SM messages with short length payload

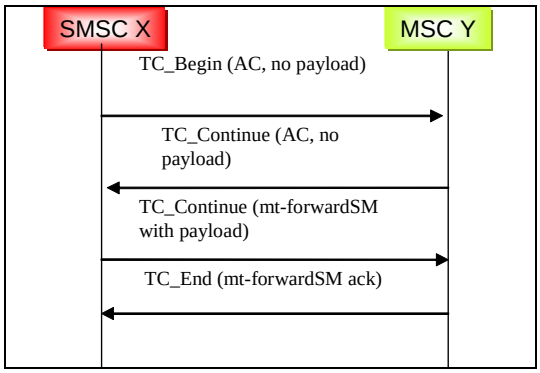

Figure 3: MAP Forward SM messages solution for long payload lengths

While the lower TCAP layer performs an implicit authentication of the originating SS7 address, this mechanism seems to be useful to prevent the SMS-fraud scenario which was described in the previous section. This can be done, if the MSC only accepts mt-forward-SM MAP messages which use the TC_Continue to transfer the MAP payload. In this case 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. Falsifying the SMSC address with a MSC address of a different network operator is not possible anymore.

Using this mechanism for address verification for the case of SMS-MO MAP signaling (mo-forwardSM) is proposed.

The advantage of this solution is that it is ready for deployment with following known restrictions: Both the SMSC and MSC need to support the exchange of MAP dialogue portions as explained above and the MSC has to enforce the use of this extended dialogue (i.e. mt-forward-SM messages without a preceding TC_Begin/TC_Continue must be rejected). This mechanism has been standardized in 3GPP TS 29.002 as an option for MAP version 2 and greater. It is believed that most MSCs do support MAP version 2, but more SMSCs might need to be upgraded.

A disadvantage is the extra load on the SS7-networks (but this might be true for other solutions as well e.g. also MAPsec adds more load on the SS7 network). Additionally, the operators must agree on this handling. The applicability of this solution towards other SMS fraud ~~scenario's~~scenarios has to be assessed. ~~)~~ Still, it is believed that a further analysis of this solution should be conducted by the 3GPP-groups that have the specialized skills (CN4 for MAP, T2 for SMS) to assess the feasibility of this solution. The fact that this solution is usable within a short term frame makes it attractive to use. Therefore it is proposed to ask CN4 and T2 for feedback. It might also be useful to inform SA2.

4 Conclusions

It is proposed to send an LS to CN4 and T2 (cc SA2), to invite them to comment on the feasibility of the proposed solution.

5 References

[SP-040279]: SA#23: Discussion paper on revitalization of MAPsec specification work

[SP-040280]: SA#23: MAPsec work item description

[S3-040492]: SA3#34: GSMA security group Report