Technical Specification Group Services and System Aspects **TSGS#24(04)0279**
Meeting #24, Seoul, South Korea, 7 - 10 June 2004

Title: **Revitalization of MAPsec specification work**
Release: Rel-6
Agenda item: 7.3

Source: T-Mobile, Vodafone, Telecom Italia Mobile

1. Introduction

Over the last few months, some network operators have been suffering more and more from SMS fraud. There are many different flavors of what could be called “fraudulent SMS usage”. In some cases, the SCCP or MAP addresses for mobile-terminated SMS traffic are spoofed, which makes it difficult for operators to apply SMS spam protection rules and may cause inter-operator accounting discrepancies.

2. Problem description and discussion

Delivering a mobile terminated SM is a procedure of two steps:

(1) The SMSC to which an originating short message was delivered interrogates the recipient’s HLR via the MAP message *Send Routing Information for Short Message* (sendRoutingInfoForSM). In response to the offered recipient’s MSISDN, the SMSC (provided that this MSISDN represents a valid subscription) receives that recipient’s IMSI and the currently valid MSC address.

(2) The SMSC then sends the short message itself to that MSC address via the MAP message *Forward Short Message* (mt-forwardSM). 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.

These two MAP operations are not interlinked; both can be run independently of each other. Therefore, it is possible to build a database of MSISDN/IMSI/MSC number entries by repeating step (1) over large MSISDN ranges. The interrogated HLR will sort out all MSISDNs not representing an existing subscription, and a significant proportion of correlated MSC numbers can be considered almost always correct since they represent the respective customers’ home areas.

In a typical SMS fraud scenario, step (1) is done as described, but for step (2) the source SMSC address is spoofed by inserting, for instance, another network’s SMSC address. The faking party’s intention is to distribute a huge number of SMs to as many people as possible; the short messages themselves urge the recipients to call some premium rate number with some kind of promise (e.g. they've won a prize). Of course, some of the SM recipients do actually call the number, and by this, the fakers of the short messages make their money. A side effect of such a procedure, perhaps not intended by these SMS spoofers, 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.

Of course, network operators suffering from such problems are eager to find out what their options are in order to suppress SMS fraud. It is clear that the design of SS7 doesn’t allow any countermeasures; SS7 is effectively based on trusted relationships within the SS7 community and as such doesn’t prevent anybody with access to the international SS7 network from injecting signalling messages with spoofed content.

Three ways of how to effectively combat SMS fraud have been proposed:

(1) SS7 over IP (SIGTRAN) plus the use of appropriate security techniques (e.g. IPsec based on the profile specified in 3GPP TS 33.210)
The superiority of such an implementation is that it allows for full end-to-end encryption, including the MAP payload itself, as is the case with MAPsec, but also the SCCP addresses too.
However, there are some drawbacks with SIGTRAN:
- the standardization process within the IETF, although very much progressed, is not yet completed,
- in general, the readiness of mobile operators to install SIGTRAN based signalling overall is still very small, and this is not likely to change very much in the near future.

(2) MAP Application Layer Security (MAPsec) has been specified for Rel-4 (3GPP TS 33.200). However, this specification is incomplete:
- MAPsec defines protection profiles combining specific groups of MAP messages and correlated protection modes to be applied by the involved components. However, the existing specification does not deal with SMS-related MAP operations of sendRoutingInfoForSM or mt-forwardSM.
- The Ze interface for the automatic key management between the Key Administration Center (KAC) and the MAP Network Elements has been started within Rel-5 (cf. SP-020115; SA#15) but was never completed and therefore removed later on (cf. SP-020709; SA#18) from the Rel-5 version of 3GPP TS 33.200. There was some expectation that the matter might be picked up again within Rel-6, but this hasn't happened so far, due to little pressure from the network operators – apparently, this is changing.

It is assumed that defining an SMS-related MAP protection profile is a minor issue. Continuing and completing the work on the Ze interface admittedly means major workload.

(3) Correlation between sendRoutingInfoForSM and mt-forwardSM
It has been proposed to link *sendRoutingInfoForSM* and *mt-forwardSM* for a specific short message by
- replacing the MSC number returned in sendRoutingInfoForSMAck by an MSRN (or other short-time-to-live token) to be provided by the VLR; this effectively limits the time span between the SRI and the actual short message itself,
- replacing the MSISDN used in mt-forwardSM by this very same MSRN.

This approach is specifically tailored to combat just one SMS fraud case as outlined above and implies significant changes to quite a number of network entities. In addition, the quality of this approach depends on the (never standardized) MSRN allocation method applied by the MSC/VLR. It appears that after some discussion there is only little interest in progressing this proposal.

Proposal (3) has several disadvantages. The mechanism seems cumbersome because of the need for the VLR to allocate an MSRN (or similar) and provide it to the HLR. This may require new MAP operations between the VLR and the HLR. The mechanism would also increase the signaling load significantly. Problems are also likely to occur because the mechanism has to deal with concatenated SMs, and with permitted standalone uses of the *sendRoutingInfoForSM* message, e.g. in MMS MM4 "determination of destination customer's PLMN". Finally, compared with proposals (1) and (2), proposal (3) only addresses a narrow range of possible SS7 abuses or frauds. For these reasons proposal (3) is not recommended.

Proposal (1) alone is not sufficient, since SIGTRAN deployment will only occur in "islands" for the foreseeable future. Therefore, proposal (1) would need to be provided in combination with proposal (2) for it to be effective. Even without support for Ze interface, it may initially be possible to deploy MAPsec in "gateways" which combine both KAC and MAP network element functionality. These gateways could be used to protect inter-operator communications, or to interconnect (secure) SIGTRAN islands.

3. Proposal
It is proposed to update and complete 3GPP TS 33.200 for Rel-6.

4. Actions

To WG SA3:

- create a MAPsec protection profile for SMS-related MAP operations,
- complete the Ze interface for automatic MAPsec key exchange between the KAC and the affected MAP Network Elements.