3GPP TSG SA WG3 Security — S3#37 **S3-050106**
21 - 25 February 2005
Sophia Antipolis, France

3GPP TSG-SA WG4 Meeting #37 **S3-05xyz**
Sophia-Antipolis, 21.-25. Feb. 2005

Source: **Vodafone**

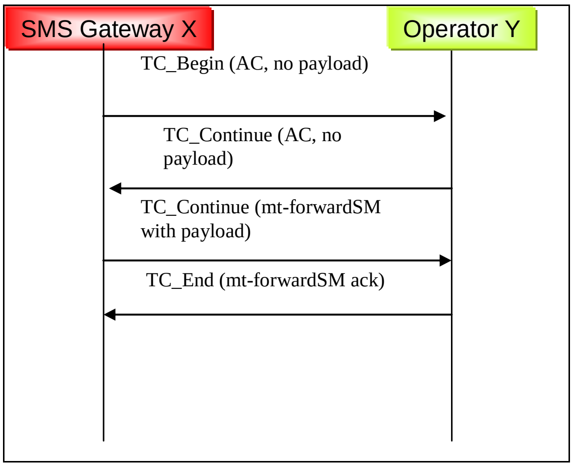
Title: **Addressing limitations of TCAP handshake for SMS transfer**

Agenda item: **6.2**

Document for: **Discussion**

1 Problem statement

TCAP handshake is specified in TS 33.200 Annex C and TS 29.002 section 23.3 as a method to prevent an attacker from masquerading as an originating network when sending an mt-forwardSM message towards a terminating network. TCAP handshake for mt-forwardSM, as illustrated in the figure below, provides a limited level of authenticity of the originating network towards the destination network using the following mechanism: If the terminating network receives an mt-forward-SM message which uses the TC_Continue to transfer the MAP payload, then it is guaranteed that the SCCP calling party address of the (empty) TC_Begin message is authentic, otherwise the first TC_Continue message would be sent to the spoofed address. The correct message flow is guaranteed by the TCAP transaction capabilities (use of Transaction identifiers).


SMS Gateway X
Operator Y
TC_Begin (AC, no payload)
TC_Continue (AC, no payload)
TC_Continue (mt-forwardSM with payload)
TC_End (mt-forwardSM ack)

There are some ways that an attacker may try to circumvent the TCAP handshake mechanism. One approach is that the attacker might be able to spoof the second TC_Continue towards the terminating network if he can guess the TCAP transaction identity that the terminating network sent to the spoofed network in the second TC_Continue. This might be possible if the terminating network allocates TCAP transaction identifiers in a predictable way.

A transaction identifier guessing attack needs to be carried out within a relatively small time window. This is because the spoofed network will return a TC_Abort to the destination node. The attacker must ensure that the destination network receives a TC_Continue, with a correctly guessed transaction identifier, before the TC_Abort from the spoofed network is received. Otherwise, the attacker must block the first TC_Continue sent to the spoofed network, or suppress or delay the TC_Abort sent from the spoofed network.

TS 33.200 V600 specifies that the destination node may use mechanisms to further enhance the unpredictability of the destination TCAP transaction identifier which needs to be included in the second TC_Continue. We believe that this is too vague and that the specifications should be enhanced to ensure that the TCAP handshake mechanism cannot be easily circumvented.

2 Solutions

2.1 Unpredictable TCAP transaction identifiers

The first solution is to impose mandatory minimum requirements on the unpredictability of the TCAP transaction identifier. The following formulation could be used:

> *The receiving node shall use mechanisms to ensure that the destination TCAP transaction identifier which needs to be used within the third message is predictable with a probability of less than 1/1000 for a third party knowing all previous TCAP transaction identifier values.*

The probability of 1/1000 is selected to ensure that the overhead for an attacker to mount a successful attack is sufficiently large (i.e. he would have to send 100 Million TCAP messages in order to deliver 100,000 fraudulent SMSs), whilst ensuring that a relatively simply allocation scheme could be used for the 32 bit TCAP transaction identifier. It is also specified that the attacker is assumed to know all previous TCAP transaction identifiers. This is done because a less stringent, but more realistic assumption would be very complicated to specify. Furthermore, it should be relatively easy to address the 1/1000 unpredictability requirement even in the unlikely event that the attacker does know the sequence of all previous TCAP transaction identifiers that were issued by the node. If this approach is selected then an example TCAP transaction identifier allocation scheme meeting the above unpredictability requirement could be included in the specifications.

Impact on destination node:
It may be difficult to modify existing TCAP transaction identifier allocation schemes to meet unpredictability requirement. It should be consider whether to specify the probability figure in the form 1/2^n.

Security considerations:
The 1/1000 unpredictability requirement ensures that the attack is not cost effective, or that the source of the attack could be detected if an attack is attempted. Example schemes may need to be developed to help implementators meet the probability requirement. History has taught us that this is not so easy to meet (cf. TCP sequence numbers). Further discussion may be needed to agree the probability figure. A higher probability may be sufficient to ensure that the attack can be detected by the target destination network.

2.2 Delayed handling of TC_Continue at destination network

An alternative approach is to delay the handling of the second TC_Continue at the destination node to give the destination network a chance to receive a TC_Abort from a spoofed network before accepting the TC_Continue. If the delay is sufficiently long then an attacker will be unable to send a TC_Continue, with a correctly guessed transaction identifier, that would get accepted by the destination node. 1 second is believed to be a sufficient delay to mitigate the attack. TC_Continue messages with incorrectly guessed transaction identifiers would get automatically rejected.

Impact on destination node:
A small change to TCAP handling needs to be made (and possibly an internal timer added). Possibly buffer sizes may need to be increased to handle the storage of pending TC_Continue messages. The processing time of all SM is increased by approximately this 1 second waiting time.

Security considerations:
An attacker could in theory block the first TC_Continue sent to the spoofed node, or suppress or delay the TC_Abort sent from the spoofed node, in order to get a TC_Continue with a correctly guessed transaction identifier accepted by the destination node. In practice this attack might be very difficult to launch (but it is difficult to be certain about this).

3 Discussion and proposal

Both solutions are considered to offer an adequate level of security given the constraints of the TCAP handshake mechanism. CN4 are asked to evaluate the feasibility and impact of the proposed solutions and provide feedback and comments to SA3. The following approaches are foreseen:

1) Mandate one of the proposed solutions
   This option should be taken if one solution is clearly better than the other from the point of view of feasibility and impact on existing entities.

2) Specify the two solutions and mandate that one of them should be implemented, but do not specify which one.

This option should be taken if both solutions are of similar feasibility, or if the feasibility depends on existing vendor-specific implementations. This option is implemented in the CR provided in S3-050051.

3) Specify the two solutions and mandate that one of them or an equivalently-secure alternative should be implemented.
This option should be taken if it is felt that vendors should be given the freedom to implement alternative solutions.

If the unpredictable TCAP transaction identifier mechanism is pursued, then CN4 should be asked to comment on the probability value. Could a lower value than 1/1000 be selected for the mechanism to remain effective? Should the probability figure be specified in the form 1/2^n?

If the delayed handling of TC_Continue mechanism is pursued, then CN4 should be asked to comment on the delay figure. Is 1 second an appropriate value to use? Should the delay figure be configurable?

Although this document is focused on applying TCAP handshake to mobile terminated SMS transfer, we believe that the problem and solutions described in this document are equally applicable if TCAP handshake is also applied to mobile originated SMS transfer.