**3GPP TSG SA WG3 Security — S3#17** **S3-010070**

**27 February - 02 March, 2001**

**Gothenburg, Sweden**

| | |
|---|---|
| **Source:** | **Nokia** |
| **Title:** | **GSM ciphering capability protection in UTRAN** |
| **Document for:** | **Discussion** |
| **Agenda Item:** | **6.2; 10.1** |

In an LS from RAN2 to S3 (=R2-010755) several questions were asked about the protection of GSM ciphering capability on the UTRAN side. This refers to the CR to 33.102 (S3-000729) and an accompanion CR was discussed in RAN2 (R2-010574 CR 676r1 to 25.331). The CR was postponed in RAN2 because there were not enough information about the security threat involved. In this document a threat scenario is described and the importance of implementing the mechanism in R99 is emphasized.

Another issue that caused confusion in RAN2 was the fact that in CR to 33.102 also RANAP signalling was changed while in CR to 25.331 the change to RRC signalling was presented as sufficient. The reason for this latter mismatch is the fact that recent advances in RRC specification implied that the relevant GSM Classmarks CM2 and CM3 are optionally transmitted to RNC also (and not only to the CN), see the LS R2-010755. In particular, this implies there is no need for change in RANAP and the change in 33.102 in RRC:security mode command is also sufficient. A corrective draft CR reflecting this is presented to S3.

An example threat scenario is the following. There is a "man-in-the-middle" node between UE and the network which acts as a simple relay but occasionally tries to modify messages in such way that some unfortunate situation occurs. In UTRAN, the man-in-the-middle cannot modify those messages that are integrity protected. However, for instance, the first RRC signalling messages are not integrity protected since the keys are not yet in place.

The object of the man-in-the-middle in our scenario is to enforce a state of affairs where the true GSM ciphering capability is downgraded when stored on the network side. Assume the network asks for the GSM classmarks CM2 and CM3 in the RRC CONNECTION SETUP message. The man-in-the-middle blocks out this question in downlink and, thus, UE does not know that it should send the classmarks. Subsequently, in the uplink message RRC CONNECTION SETUP COMPLETE, the man-in-the-middle adds classmarks with downgraded ciphering capability information. An alternative way is to simply modify the classmarks in uplink signalling.

The impacts of the threat will increase with the introduction of the A5/3 ciphering algorithm as part of the terminal base will support this stronger algorithm while the rest support only A5/1 and A5/2. As integrity protection is in use in UTRAN it is useful to extend the protection also to GSM part as regards handovers from UTRAN to GSM.

What is proposed in RAN2 is to add the GSM ciphering capability (7 bits) to the RRC: SECURITY MODE COMMAND just as UTRAN security capability is added in the same message to protect it from the man-in-the-middle attack. The UE checks the correctness of this information.

Another way to protect the GSM ciphering classmarks would be to use the specific (integrity protected) RRC UE capability information procedure referred to in the LS from RAN2 . However, this cannot be mandatory (prior to inter-system handover) since the other method to obtain the classmarks (in RRC connection establishment) was introduced to decrease the signalling load. Hence, this other method should also be protected.

Let us now discuss what are the consequences if the change is postponed to later releases. In that case, if either the UE is R99 or the network is R99 the protection mechanism does not work: either the network does not send the capability information downlink or the UE does not check the correctness of the information. Consequently, for instance, a R99 network cannot protect the A5/3 capability in the UE when handover to GSM BSS (with support to A5/3) occurs.