3GPP TSG SA WG3 Security — S3#19 **S3-010399**

3 - 6 July, 2001

Newbury, UK

Source: **SA3**

Title: **On the use of Network Domain Security for protection of SIP signalling messages**

To: **SA2, CN1 and CN4**

Contact Person:

Name: Greg Rose

E-mail Address:ggr@qualcomm.com

Tel. Number: +61 2 9817 4188

On the use of Network Domain Security for protection of SIP signalling messages

SA3 has for some time now made the assumption that Network Domain Security for IP (NDS/IP) ought to be used to protect the privacy of IMS SIP signalling messages in the core network. It has seemed to be desirable to reuse the already defined mechanisms for protection of the lower IP layer defined in NDS/IP as defined in draft TS33.210 (S3-010303). Note that other mechanisms are used to protect the integrity of the SIP messages.

However, the IMS SIP messages are currently carried within GTP-U messages in the core network and another working assumption has been that GTP-U messages are not encrypted in NDS/IP.

The decision whether or not to apply IPSec protection to a particular packet is based on the destination IP address and port number. But since the original SIP registration message is tunnelled in GTP-U, which has a defined port number, there is no simple method to decide whether or not to encrypt a particular GTP-U packet.

In other words, the two working assumptions above are somewhat in conflict.

Some alternatives identified for the problem

So with this as the background SA3 kindly asks for some advice on how to solve this problem since we are still of the opinion that NDS/IP should be the preferred means of protection for IMS SIP in the core network. We have identified five possible option and these are:

1. To not encrypt any GTP-U messages, understanding that this means that IMS SIP messages will not be encrypted in the core network.
2. To protect all GTP-U messages, including the small proportion that are IMS SIP messages.
3. To introduce a new sub-version of GTP for the IMS control plane (GTP-IC). This new GTP-IC would then have a unique port number assigned to it, enabling those messages to be encrypted. All IMS control plane messages would then have to be tunnelled through GTP-IC in the core network.

4. Extend GTP-C to contain all IMS control plane messages. All IMS control plane messages would then have to be tunnelled through GTP-C in the core network. Again, since GTP-C is always encrypted, the IMS SIP messages would be encrypted.
5. Introduce multiple IP addresses (multi-homing) of the CSCFs such that GTP-U containing IMS control plane messages would use a different set of IP addresses from the GTP-U containing non-IMS control plane messages.

Option 1 is not preferred because SA3 believes that signalling messages should, in general, be protected.

Option 2 is acceptable from a security viewpoint, but may be considered to be too inefficient.

When it comes to evaluating options 3-5 SA3 recognizes that this is largely outside our scope. We would however like to point out that multi-homing and IPsec don’t go particularly well together. So we recommend that option 5 not be seriously considered.

SA3 has not identified any important security differences between option 3 and 4, but it would seem conceptually cleaner to have a separate GTP subversion for the IMS control plane and this will also open the possibility of having different security policies for the current GTP-C and IMS control plane messages (GTP-IC). However, either option 3 or 4 will be acceptable to SA3.

Conclusion

First it is necessary to decide whether IMS SIP messages need to be protected within the core network at all. SA3 continues to assume that this is desirable.

In particular, SA3 asks for an investigation of the possibility of having either the IMS SIP messages to be transported within GTP-C or to have a new subversion of GTP (GTP-IC), which will be dedicated to tunnelling of IMS control plane (SIP) messages.

To be able to progress work on TS 33.203, SA3 will continue to keep its current working assumption that NDS/IP can be used for protection of IMS SIP messages.

Should the investigation conclude that neither of the options is feasible, SA3 would probably have to revisit its decision to use NDS/IP for protection of IMS SIP messages. This again is likely to introduce delays in SA3 progress on TS 33.203.