3GPP TSG SA WG3 Security — S3#19 **S3-010393**

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: Geir M. Køien

E-mail Address:geir-myrdahl.koien@telenor.com

Tel. Number: +47 3725 4952

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 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 TS33210 (S3-010303).

However, the IMS SIP messages are currently carried within GTP-U messages in the core network and this makes it difficult to use NDS/IP.

The root of the problem is due to the fact that GTP-U as a tunnelling protocol stores the IP addresses and portnumbers of its target protocol/packet within the payload of GTP-U. NDS/IP is closely based on IPsec and the IPsec packet-processing rules also apply to NDS/IP. IPsec will only inspect the source/destination IP address, the source/destination portnumbers and the protocol-id to determine whether or not IPsec is to be applies to the packet. So this means that when processing a GTP-U packet IPsec will **only** see the GTP-U IP header. There is no way IPsec (and NDS/IP) will be able to handle an IMS SIP message contained within a GTP-U packet any different from the other GTP-U packets. The possibility of extending the IPsec processing rules to also inspect the payload have been investigated and found not to be practical due to the significant processing overhead incurred.

This leaves us in a situation where protection of IMS SIP will require all GTP-U messages to be protected. This is an undesirable situation since the volume of GTP-U packets is likely to be high.

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 four possible option and these are:

1. To protect all GTP-U messages
2. To introduce a new sub-version of GTP for the IMS control plane (GTP-IC). This new GTP-IC would then have a unique portnumber assigned to it. All IMS control plane messages would then have to be tunnelled through GTP-IC in the core network.

3. 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.
4. Introduce multiple IP addresses (multi-homing) at 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.

SA3 have already considered protecting GTP-U and has come to the conclusion that it would be unrealistic to require protection of all of GTP-U.

When it comes to evaluating options 2-4 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 4 not be seriously considered.

SA3 has not identified any important security differences between option 2 and 3, 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 difference security policies for the current GTP-C and IMS control plane messages (GTP-IC). However, both option 2 and 3 will be acceptable to SA3.

Conclusion

NDS/IP has been selected as the mechanism of choice for protection of IMS SIP messages in the core network. A problem has been identified in applying NDS/IP for protection of IMS SIP messages since IMS SIP is carried as payload in GTP-U. Due the IPsec packet processing rules one is left with the choice of either protection all of GTP-U or not at all.

Since this is not acceptable, other solutions must be sought.

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 dedicate to tunnelling of IMS control plane 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.