3GPP TSG SA WG3 Security — S3#19 **S3-010389**

3 - 6 July, 2001

Newbury, UK

Source:	**Telenor**
Title:	**On the use of Network Domain Security for protection of SIP signalling messages**
Document for:	**Discussion**
Agenda Item:	**7.3**

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

We have for some time now made the assumption that Network Domain Security for IP (NDS/IP) should be used to protect SIP signalling messages in IMS in the core network. Provided that we want to stay with that assumption, we have some issues that must be addressed.

Protection of GTP-U

It is currently assumed that Network Domain Security for IP (NDS/IP) as specified in draft TS 33.210 shall also be used for protection of SIP messages in IMS.

Technically this is fully possible, but it is at odds with the current assumption on how NDS/IP will be used. The problem is that SIP in IMS is carried within GTP-U messages, and that NDS/IP currently do **not** protect GTP-U.

Now it would be fairly easy to change TS 33.210 to also accommodate GTP-U. However, with the normal IPsec processing rules it will not be possible to inspect the contents of GTP-U to discriminate between SIP signalling contained within GTP-U and other user data. NDS/IP uses IPsec in its intended way, and consequently there is no easy way to separate SIP signalling from other data in GTP-U. So unless one wants to extend the IPsec (NDS/IP) processing rules to inspect the payload contents of the packets one is left with the choice of either protect all of GTP-U or nothing. It must be said that it is **not** a good idea to change the processing rules since the performance overhead of inspection all GTP-U packets would likely be formidable.

Now to protect all of GTP-U might seem to be the desirable choice, but one should be aware that this involves protection of rather large amounts of data. This will probably take dedicated HW equipment and may introduce delays to services.

How to distinguish IMS control plane from user data

To blindly protect all of GTP-U might not be desired and it also leaves a lot to be desired in terms of protection granularity. So it might be better to find ways to try to distinguish IMS control plane signalling from other user data in GTP.

There seems to be two ways of doing this that is compatible with the IPsec processing rules:

1. *Distinguish IMS control plane traffic by having a dedicated GTP portnumber for it.*

This would in effect introduce a new sub-version of GTP. The new GTP might then be called GTP-IC (for IMS Control plane). This alternative is clearly feasible, but will require changes at least to 23.060 and 29.060 and thus require the cooperation of SA2 and CN4.

2. *Distinguish IMS Control plane traffic by having separate IP addresses for it.*

   This would in effect require that the hosts be multi-homed. So an NE would then have to maintain two IP addresses and use one of them exclusively for IMS control plane traffic. After a brief consultation with some CN1 delegates this seems to be possible from their point of view provided that a separate PDP context is used. The question of multi-homing is tricky with IPsec and its questionable whether this solution can actually be developed to a workable alternative.

Conclusion

Under the assumption that NDS/IP is to be used for protection of IMS SIP signalling messages we must either:

a) Protect all of GTP-U (very coarse granularity)

b) Separate IMS control plane messages from other user traffic by introducing GTP-IC (distinguishing by means of separate portnumbers for GTP-U and GTP-IC)

c) Separate IMS control plane messages from other user traffic by introducing multi-homing (distinguishing by means of separate IP addresses for IMS control plane and user data)

   (multi-homing might not be compatible with IPsec)

From a technical perspective I would recommend the approach outlined in b). However, we must probably seek the advice from SA2, CN1 and CN4 to progress this matter.

The first action would probably be for us to send a liaison statement to the above-mentioned groups to outline the problem.

/Geir M. Køien