3GPP TSG SA WG3 Security — S3#33 ***Tdoc ⌘S3-040357***
10 - 14 May 2004, Beijing, China

Source: Nokia

Title: **Privacy handling for Rel-6**

Document for: Discussion/Decision

Agenda Item: IMS

1. Background

The interworking with non-IMS network is specified in TS 33.203 section 6.5. It describes the TLS shall be used to protect traffice over Mm interface, and guarantee the trust relationship with a non-IMS SIP service provider. However the CSCF misses the criteria to identify whether the destination/source is trusted, due to the Rel-5 IMS lack of mechanism to identify the trust relation with other end. This contribution is a follow-up work for resolving the privacy handling of Rel-6 IMS when interworking with whatever networks.

2. The Problem description

The solution in TS 33.203 section 6.5 resolved the security protection, from a CSCF point of view, of the open link (Mm interface) connected to the non-IMS network. An IMS CSCF is able to discover the TLS capability of a SIP proxy before connection is established. If TLS is not supported in the next hop, then the network is untrusted. If TLS is supported, the IMS SIP proxy request a certificate from the other SIP proxy. And once the TLS connection is established, the IMS can tell that the other end is trusted. Therefore the user required privacy can be handled accordingly.

It was suggested in the NOTE in section 6.5, that NDS/IP specified in TS 33.210 shall be used to protect the SIP signalling when interworking between IMS networks. In other words, a CSCF shall deploy different protections triggered by the criteria whether the destination/source is an IMS or non-IMS network. So the issue rising up is: how can a CSCF conclude whether the destination/source is an IMS or non-IMS network before any protection is deployed?

Rel-5 IMS does not attempt to understand the other end; it just blindly trusts all connected networks. It is only based on the connectivity of the SGW to transfer the SIP signalling. If the SGW is missing, the SIP signalling is just dropped. Due to the usage of Security Gateway (SGW) is in different layer as the transport layer (SIP), the CSCF cannot detect the SIP message is unprotected. As the consequence, if an IMS bypasses the IPsec protection, a receiving CSCF is not able to detect that. Therefore the NDS/IP only provides the protection to the signalling, but it doesn't help a Rel-6 CSCF to recognize the existence of trust relationship, i.e. it doesn't provide means to logic judgement.

Further issue presents when Rel-6 IMS CSCF speaks with an Internet proxy. Before TLS connection is established, the unprotected SIP messages also pass thought the SGW. Thus a CSCF cannot trust the other end simply because the traversal of SGW.

Therefore with current network topology a CSCF cannot conclude whether the destination/source is an IMS or non-IMS network before any protection is deployed. New solution is needed for interworking of IMS networks so as to identify the trust relationship with the other end.

3. The general solution for interworking

This section provides a solution to the issue presented in section 2. It is proposed that each CSCF to store a list of IMS trusted domains that have signed interworking agreement. As the consequence, the CSCF when sending and receiving a SIP message, shall sort the domain name of the other end from the trust domain list, together with the security parameters visible in a certificate (e.g., certificate authority, common name or organization). The CSCF can identity an IMS that is not on the list as an untrusted network. However this does not differentiate an untrusted network is IMS or non-IMS.

We propose to use TLS solution for IMS interworking so as to resolve the trust relation problem. If the request is not received via TLS, the sending SIP CSCF is not trusted. If the request is sent via TLS, the IMS SIP proxy request the sending SIP proxy a certificate. Then the IMS SIP proxy verifies the certificate against the list of trusted networks, determining whether the sending SIP proxy is trusted or not.

Additionally, each IMS network configures the DNS NAPTR/SRV records to give higher preference to TLS over UDP, TCP, SCTP (or other transport protocols) for the SIP service. This allows an IMS network to always try first TLS as a transport protocol.

As the consequence, SIP traffic through GTP-U plane does not need to be IPsec protected. Rather it is based on the end-to-end TLS connection. Therefore the NDSP/IP is not repeatedly used underneath of transport layer.

4. Suggested change over Rel-5 IMS Privacy

Based on the solution discussed in section 3, a proposal of change is shown below. It is written against the CR for Rel-5 SIP privacy (S3-030600), for convinence of the audience. In the companion CR against TS 33.203 v6.2.0, the same texts are shown but all in revision mark.

It is also proposed to upate the section 5.6 to the general case which is applicable to both IMS and non-IMS interworking.

5.3 SIP Privacy ~~for IMS Networks~~

Privacy may in many instances be equivalent with confidentiality i.e. to hide the information (using encryption and encryption keys) from all entities except those who are authorized to understand the information. The SIP Privacy Extensions for IMS Networks do not provide with such confidentiality. The purpose of the mechanism is rather to give an IMS subscriber the possibility to withhold certain identity information of the subscriber as specified in [22] and [23].

NOTE 1: It is useful that the privacy mechanism for IMS networks does not create states in the CSCFs other than the normal SIP states.

~~The IMS Network shall, from the Privacy function point of view, be a closed network by the implementation of Security Gateways for IMS signalling as defined in TS 33.210 [5].~~

~~NOTE 2: In particular when a SIP message is routed through the SEG towards an IP address, which is not operating the Za interface, i.e. there is no SA available in the SEG for applying IPsec ESP the SEG will, in compliance with TS 33.210 [5], drop the packet.~~

When a Rel-6 IMS interworking with a foreign network, the CSCF in IMS network shall decide the trust relation with the other end, based on whether the security mechanism for the interworking (cf. section 6.5) is applied as well as the availability of an inter-working agreement. If the interworking network is not trusted, the privacy information shall be removed from the traffic towards to the foreign network. When receiving SIP signalling, the CSCF shall also verify if any privacy information is already contained. If the interworking network is not trusted, the information shall be removed by the CSCF, and retained otherwise.

5. Proposal to SA3

It is proposed to SA3 to endorse the companion CR against TS33.203 v6.2.0.