3GPP TSG SA WG3 Security — S3#20 **S3-010512**

16 - 19 October, 2001

Sydney, Australia

3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010118**

14 September, 2001

Sophia Antipolis, France

Source: **Hutchison 3G UK**

Title: **Confidentiality of SIP signalling between UE and P-CSCF**

Document for: **Discussion/Decision**

Agenda Item:

Introduction

Following on from the LS on GTP-IC, we were looking at the provisioning of confidentiality between UE and P-CSCF, in particular the working assumption from Madrid.

Problems with the Working Assumption

We are not convinced that relying on NDS for confidentiality on the UE-PCSCF leg is a good decision for the following reasons:

1) Loss of access network independence: To have the option of confidentiality, the user must be using a 3G network to access IM services. Furthermore that network must have an IM domain or at a minimum recognise the mechanism to protect SIP signalling (not all networks would be upgraded at the same time). This does not follow the basic principle that services should be transparent to the transport network. Whether confidentiality is applied should depend entirely on the IM domain and not rely on the access network. We do not want to be in the same position as with MAP that requires everyone to have updated their network before we can guarantee to provide security.

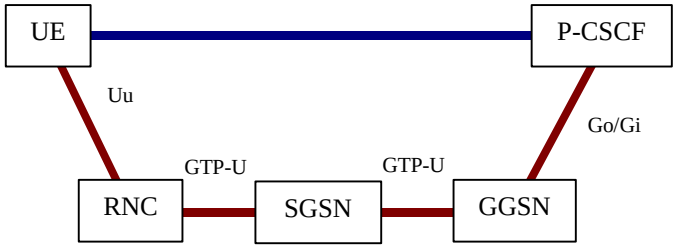
2) Amount of ciphering: Encryption/decryption between the following is needed to provide confidentiality between the UE and the P-CSCF:

Encryption between UE and RNC (probably already performed).

Encryption on GTP-U/GTP-IC between the RNC and SGSN and between the SGSN and GGSN.

Encryption on Gi/Go between GGSN and PCF/P-CSCF. NDS would have to be extended to the Gi/Go interface (this shouldn't be a major issue).

This seems to be an excessive amount of ciphering.



The solution to these concerns is to provide confidentiality between UE and P-CSCF at the SIP or upper IP layer (i.e. UE and P-CSCF terminate the encryption). This fits in better with the concept of the IM domain being independent of the PS domain. The encryption key Ckim, which is already negotiated during the IM authentication could be used. Since we are applying the integrity mechanism at the UE and P-CSCF, confidentiality could be applied at the same level without much more effort.

The only disadvantage is that this is putting more work onto the UE, i.e. it is now responsible for both integrity and ciphering (currently optional). This is a small disadvantage compared to the disadvantages given above for using NDS to provide the security.

Conclusion

In conclusion we believe the only viable place to provide confidentiality for SIP signalling is at the UE and P-CSCF, not hop by hop at the intervening network elements. We propose that this should be the SA3 position.

Actions Required

If this is agreed for SA3, the following changes (or something similar) will be needed to TS 33.203.

Section 4 Overview of security architecture

Figure 2 – the interfaces should not be given as Zc. There is very little need to show the GSNs etc.

Section 5.1.2 Confidentiality protection.

Confidentiality protection shall optionally be used between the UE and P-CSCF for protecting SIP signalling. The following mechanisms are provided.

1. The UE and P-CSCF shall negotiate what confidentiality algorithm shall be used for the session.
2. The UE and the P-CSCF shall agree on a confidentiality key CK_{IM} that shall be used for the confidentiality.

Section 5.1.3 Integrity Protection

The method to provide integrity should easily extend to provide confidentiality (unless it is decided that confidentiality is not needed).

Section 6.2 Confidentiality Mechanisms

Remove “ and Network Domain Security [5].”