3GPP TSG SA WG3 Security S3-010073

Meeting S3#17

Göteborg, 27 Feb – 2 Mar, 2001

Source: Siemens AG

Title: Summary of arguments and proposal for a decision on location of security functions

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

Two alternative proposals for an IM domain security architecture were presented at S3#16 by Ericsson in TD S3-000699 and by Siemens in TDs S3-000689 and S3-000753. This document sums up the arguments from these previous contributions taking into account the new arguments from two companion contributions by Siemens presented to S3#17.

1 Introduction

This document will not repeat the documents introduced in S3#16. For details please refer to these.

The questions under discussion regarding the location of security functions are:

- Which network entity should perform the final check in the authentication and key agreement (AKA) protocol with the UE for SIP registration of a (roaming) user, the P-CSCF or the HSS?
- Which network entity should terminate the access confidentiality protection of SIP messages sent from/to the UE?
- Which network entity should terminate the access integrity protection of SIP messages sent from/to the UE?

We answer these three questions in the order in which they seem easiest to agree.

2 Location of confidentiality function

There is agreement in S3 that the confidentiality function which encrypts and decrypts SIP messages sent to and from the UE should be located in the P-CSCF.

3 Location of integrity function

Here, there are both security and complexity arguments which point to the same conclusion:

In the companion contribution S3-010Si1, TS 23.228 was analysed from a security point of view, and it was concluded that the integrity function which checks the integrity of SIP messages sent to and from the UE should be located in the P-CSCF. (AT&T's contribution S2-010512 came to the same conclusion.)

In addition, there are the complexity arguments already mentioned in earlier contributions: If the integrity functions was to be located in the S-CSCF then two types of nodes would have to be equipped with cryptographic functionality (probably with HW support) and with user databases holding the cryptographic keys, namely the P-CSCF for confidentiality and the S-CSCF for integrity. This increases complexity, both for implementation and for operation and maintenance. It also raises security issues, as the more complex a system is the more likely it is to fail, and the more widely distributed security functionality is the more difficult it is to protect.

Availability of mechanism: the UE can address the P-CSCF at IP layer (this needs to be corroborated by S2). So, if integrity terminates in the P-CSCF then IPSec is available as a candidate for the integrity mechanism. (But an application layer integrity mechanism would not be precluded.) If integrity terminates in the S-CSCF then an application layer integrity mechanism is needed. The integrity mechanisms specified in RFC2543 are not suitable for use in the IM domain, cf. S3-000447 and S3-000700 (TR33.8xx). So, a new mechanism would have to be defined.

For the above reasons, the integrity function should be located in the P-CSCF and not in the S-CSCF.

4 Location of final authentication check

This decision is less obvious than the previous ones. It is a trade-off between an obvious reduction in complexity and an (in our judgement) less obvious gain in security:

There is a clear reduction in complexity for the HSS if the final authentication check (RES = XRES?) can be performed in the P-CSCF because then the HSS simply has to respond to a query by the I-CSCF. If instead the final authentication check is performed in the HSS then the HSS needs to maintain user states during a protocol run, increasing its load.

This increase in complexity is significant, and the alternative solution should be chosen only if there are strong security requirements necessitating it.

5 Network domain security

It was shown in the companion contribution S3-010Si1 that messages sent between IM domain nodes need to be protected. This should be done according to the principles laid down for native IP-based protocols in TS 33.200 "Network Domain Security".

6 Conclusion

- Locate confidentiality and integrity functions in the P-CSCF
- Perform final authentication check in the P-CSCF
- Apply Network Domain Security according to TS 33.200