3GPP TSG SA WG3 Security **S3-020530**

8th – 11th October, 2002

Munich, Germany

Agenda Item: IP multimedia subsystem (IMS)

Source: Ericsson and Hutchison 3G

Title: The use of SAs in IMS user authentication failures

Document for: Discussion/Decision

1. Introduction

In IMS, use authentication may (in theory) fail in home network [TS 33.203]. Currently, the error messages related to unprotected registrations are also sent unprotected to the UE. However, the UE may not be able to trust on these messages. This document discusses the issue of sending these messages protected instead. Accompanied CR propose changes in TS 33.203.

2. Problem description

According to TS 33.203, the user authentication may fail in the home network [chapter 6.1.2.1]:

> *In this case the authentication of the user should fail at the S-CSCF due an incorrect response (received in SM9). However, if the response is incorrect, then the IK used to protect SM7 will normally be incorrect as well, which will normally cause the integrity check at the P-CSCF to fail before the response can be verified at S-CSCF. In this case SM7 is discarded by the IPsec layer at the P-CSCF.*
>
> *If the integrity check passes but the response is incorrect, the message flows are identical up to and including SM9 as a successful authentication. Once the S-CSCF detects the user authentication failure it should proceed in the same way as having received SM9 in a network authentication failure (see clause 6.1.2.2).*

This should not happen in practice because the UE has been able to authenticate the home network based on the AKA challenge in SM6. Furthermore, UE and the home network have been able to generate the same IK. UE and P-CSCF have proven this because they have been able to use the IK for protecting the message SM7.

If it does happen and if the SM1 was sent unprotected, P-CSCF will send SM12 '4xx Auth_Failure' message unprotected to the UE. However, the UE should not trust on such a message because it may have been originated from an attacker. If the UE trusts on an attacker originated message, it will remove the new SAs, and cannot receive the real SM12 message when that arrives.

P-CSCF could send the SM12 message using the new SA. This solution is also problematic because the SAs created during the registrations have not been tested towards the UE. There is no guarantee that an attacker has modified the SA parameters in SM1, and consequently that UE will ever receive the SM12 message. However, not receiving SM12 is more secure alternative than receiving unprotected SM12. The case in which SM12 is not received will probably cause some re-transmissions of SM7. However, the error case is only theoretical and may never occur in practice.

We propose that P-CSCF should always send authentication failure message to the UE protected.

3. Conclusions

We propose that TS 33.203 should rule out the case in which P-CSCF sends an error message in SM12 unprotected. Instead, such error message should be sent using the SA created during the registration.

4. References

[TS 33.203] 3GPP (2002) Access security for IP-based services (Release 5), TS 33.203 v5.3.0.