3GPP TSG SA WG3 Security#33 **S3-040264**
10 – 14 May, 2004
Beijing, China

Agenda Item: **6.1**

Source: **Vodafone**

Title: **Security for early IMS implementations**

Document for: **Discussion and Decision**

Abstract

In this contribution we consider security aspects of early IMS implementations and propose that 3GPP specify interim security features to address security requirements of early IMS implementations.

1. Introduction

3GPP IMS provides an IP-based session control capability based on the SIP protocol. IMS can be used to enable services such as push to talk, instant messaging, presence and conferencing. It is understood that “early” implementations of these services will exist that are not fully compliant with 3GPP IMS. For example, SA2 has recognized that although 3GPP IMS uses exclusively IPv6, as specified in clause 5.1 of TS 23.221, there will exist IMS implementations based on IPv4. Interworking aspects and migration scenarios for IPv4 based IMS implementations are studied by SA2 as part of TR 23.881 [23.881].

Non-compliance with IPv6 is not the only difference between early IMS implementations and 3GPP compliant implementations. In particular, it is expected that there will be a need to deploy some IMS-based services before products are available which fully support the 3GPP IMS security features defined in TS 33.203. Non-compliance with TS 33.203 security features is expected to be a problem mainly at the terminal side, because of the potential lack of support of USIM/ISIM authentication (especially in 2G-only devices) and because of the potential inability to support IPsec on some terminal platforms. This issue has been recognized by SA2 in a recent LS which asks SA3 to “provide feedback on possible security mechanisms that take into account early implementations of IMS that do not fully support TS 33.203” [S2-041674].

Although full support of TS 33.203 security features is preferred from a security perspective, it must be acknowledged that early IMS implementations will exist which do not support these features. Therefore, there is a need to ensure that simple, yet adequately secure, mechanisms are in place to protect against the most significant security threats that will exist in early IMS implementations. Furthermore, to maximise interoperability, it is important that these mechanisms are adequately standardised.

2. Requirements on interim solution

Low impact on existing entities: As stated in the LS from SA2, any early IMS security mechanisms “should be such that impacts on existing entities, especially on the UE, are minimised and would be quick to implement”. It is especially important to minimise impact on the UE to maximise interoperability with early IMS terminals. The mechanisms should be quick to implement so that the window of opportunity for the interim solution is not missed.

Adequate level of security: Although it is recognised that the interim solution will be simpler than the full 3GPP IMS security solution, it should still provide an adequate level of security to protect against the most significant security threats that will exist in early IMS implementations. As a guide, the strength of subscriber authentication should be comparable to the level of authentication provided for existing chargeable services in mobile networks.

Smooth and cost effective migration path to 3GPP solution: Clearly, any security mechanisms developed for early IMS systems will provide a lower level of protection compared with that offered by the full set of 3GPP IMS security features. The security mechanisms developed for early IMS systems should therefore be considered as an interim solution and migration to the full set of 3GPP IMS security features should take place as soon as suitable products become available at an acceptable cost. In particular, the interim solution should not be used as a long-term replacement for full 3GPP IMS security. It is important that the interim solution allows a smooth and cost effective migration path to the full 3GPP solution.

Co-existence with 3GPP solution: It is clear that terminals supporting the interim solution will need to be supported even after 3GPP compliant terminals are deployed. The interim solution should therefore be able to co-exist with the full 3GPP solution. In particular, it shall be possible for the SIP/IP core to differentiate between a subscription using interim security mechanisms and a subscription using the full 3GPP solution.

Protection against bidding down: It should not be possible for an attacker to force the use of the interim solution when both the terminal and the network support the full 3GPP solution.

No restrictions on the type of charging model: Compared with full 3GPP IMS security solution, the interim solution should not impose any restrictions on the type of charging model that can be adopted.

Standardisation of a single interim solution: Interfaces that are impacted by the interim solution should be adequately standardised to ensure interoperability between vendors. To avoid unnecessary complexity, a single interim solution should be standardised.

Support access over 3GPP PS domain: Currently the main requirement is to support secure access over the 3GPP PS domain (including GSM/GPRS and UMTS access). Access based on WLAN scenario 2, or other alternative access networks, is a lower priority at this time.

Low impact on provisioning: The impact on provisioning should be low compared with the full 3GPP solution.

3. Proposal

It is proposed that SA3 develop an interim solution for IMS security that satisfies the requirements in Section 2 above.

A proposed interim security solution is presented in a companion document [S3-040265].

References

[23.881] 3GPP TR 23.881 V0.3.0: “Interworking aspects and migration scenarios for IPv4 based IMS Implementations”

[S2-041674] 3GPP SA2 Tdoc S2-041674, Liaison from SA2 to SA3: “LS on non-compliance to IMS security”, SA2 meeting #39, Shenzhen, China, 19-23 April 2004.

[S3-040265] 3GPP SA3 Tdoc S3-040265, “Interim security solution for early IMS implementations”, SA3 meeting #33, Beijing, China, 10-14 May 2004.