3GPP TSG SA WG3 Security — S3#37 **S3-050054**

21 - 25 February 2005

Sophia Antipolis, France

Title: **Protection of Service Announcements**

Source: **Nokia**

Document for: **Discussion/Decision**

Agenda Item: **6.20**

Work Item: **MBMS**

1 Introduction

It has been noticed that the protection of the service announcement over MBMS bearer has not been considered [1]. The SA3 assumed that the service announcement is only sent using point-to-point bearers; see Threats in B.1 of TS 33.246 [2]. However, The MBMS Protocols and Codes specification includes possibility to send the service announcement over the MBMS bearer [3]. This paper presents some possible methods to protect service announcements and evaluates them. This paper also considers whether it is practical to protect service announcements or not.

2 Discussion

The protection of the service announcement can be based on the public key certificates. The use of public key certificates is a rather complex solution, because certificates require at least minimal public key infrastructure (PKI). The minimal PKI would contain the certificate authority (CA), manual certificate handling and a mechanism to check the status of certificate (e.g. LDAP and certificate revocation lists). It is impractical to use PKI to protect service announcements, because it is not used by other MBMS security functions.

The second option is to use pre-shared secrets. It is impractical to introduce a pre-shared key, which is shared between all users (UEs) and the BM-SC, because this requires either manual configuration by the user or change of SIMs/USIMs. The re-keying of shared secret is also problematic, because it would be manual operation and users would not get service announcements if they forget to update the shared secret. Please note that this kind of solution provides only limited security, because the pre-shared key is shared between multiple users i.e. other users can forge service announcement messages.

The third option is to use two-layered solution. In this solution, the service announcement is divided into two parts. In the first part, users are informed about the service announcement service using point-to-point bearers. In the second part, users join to the service announcement service and receive service announcements via MBMS bearer. The service announcement service (second part) is a normal MBMS service, but users of the service announcement service would not be charged. The security is similar to the current MBMS key delivery, but keys are

shared between multiple users i.e. other users can forge service announcement messages.

The fourth option is to bind a service announcement to the HTTP digest authentication. In this solution, the UE calculates a hash over the service announcement and the hash is bound to the authentication. The input of MRK derivation could include the hash. If a malicious user has forged the service announcement then the victim cannot join the service, because the authentication fails.

3 Conclusions

If service announcements are not protected then malicious users may forge service announcements. However, the security level is similar to the use of two-layered model and pre-shared secrets model, because these solutions share keys between all users. On the other hand, public key certificates are overkill, because it is not utilized in other MBMS security functions.

We propose that service announcements are not protected, because if an attacker can modify a service announcement then it is also possible to modify broadcast or multicast MBMS data. If the protection is required anyway then the binding model should be used, because it requires only modifications to the MRK derivation and it is more secure than pre-shared key and two-layered model.

4 References

[1] S3-041132, Issue list to complete MBMS Security, SA WG3

[2] 3GPP TS 33.246, Security of Multimedia Broadcast/Multicast Service, version 6.1.0.

[3] 3GPP TS 26.346, Multimedia Broadcast/Multicast Service; Protocols and Codecs, version 1.5.0.