3GPP TSG SA WG3 Security — S3#31 **S3-030696**
18 – 21 November 2003,
Munich, Germany

Agenda item: MBMS Security
Source: Qualcomm Europe~~, , Schlumbergerema~~
Title: Adding Integrity to Counting Idle Mode terminals in MBMS~~Progress report on MBMS 3GPP2 solution~~
Document for: Discussion and Decision

Abstract

This input document considers an MBMS security issue raised in RAN2 and GERAN2 (eg [1],[2], [3],[4]), but to date not discussed in SA3: the concern is that malicious UE may force a network operator to broadcast MBMS content when there are insufficient MBMS subscribers to warrant the broadcast. Thus an attack on network resources may be launched. This paper proposes to add integrity to the registration procedure to prevent this attack on network resources.

Introduction

At present, MBMS counting procedures for IDLE mode terminals suffer a lack of integrity protection; for example, from [4]:

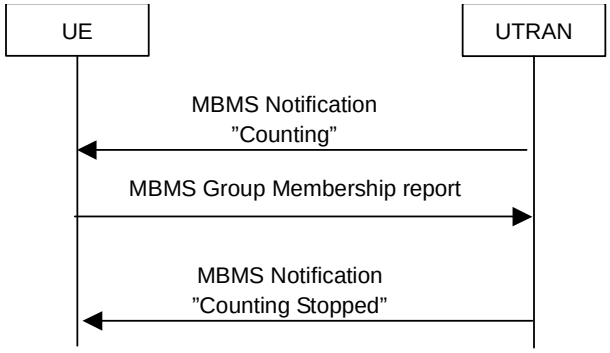
'Vodafone feel that further work may be required on the authentication of users before the start of the MBMS data transfer phase. This additional security process may be completed by a number of users on each cell and could consist of prompting a subset of MS to complete the Routing Area Update procedure so that the MS can be authenticated. There are some worries that a number of rogue handsets to (sic) reek havoc on the efficiency of the network by responding to a count where no real users are in a cell, forcing the network to provide the MBMS service in a point-to-multipoint manner to an empty cell.'

We propose a simple approach to adding integrity and avoiding this attack.

Integrity problem

The proposed signalling flow, presented below, suffers the lack of integrity of the MBMS group membership report message:

The fact that the MBMS group report is not integrity protected means the RNC is not able to decide whether a Group Membership message received is really from a user who has subscribed to a specific MBMS service.



As a result, malicious terminals could send a sufficient number of MBMS group membership report messages, forcing point-to-multipoint transmission in a cell although there are no joined UEs in that cell. Thus the integrity problem does not degrade the protection of the MBMS content but could lead to the unnecessary broadcast transmission of the data to the cell.

Proposal:

Firstly, Qualcomm proposes to consider this threat to the list of threats in 33.246.

Secondly, is proposed that this problem may be overcome as follows: upon receiving an MBMS Notification, an MS will form a response on the UICC, including its IMSI, Service_ID and the Sequence Number received in the Notification. This response will then be secured using key(s) derived from the BAK, say BAK', by encrypting the content and applying a MAC. These keys are also derived by the serving BMSC and transmitted to the RAN. The RAN can therefore determine that the response is coming from UE which is in possession of the appropriate BAK', and that the increase of the count is therefore appropriate.

References

1. R2-030120**,** Providing integrity to counting IDLE mode UE, Nokia.
2. G2-030347, Counting Requirements in MBMS, Siemens.
3. G2-030495, MBMS Subscriber Counting, Ericsson.
4. GMBMS-030012, Principles for MBMS in GERAN, Vodafone.