3GPP TSG SA WG3 Security — S3#31 **S3-030701**
18 - 21 November 2003
Munich, Germany

Source: **Siemens**

Title: **MBMS: Replaying of RAND values**

Document for: **Discussion and decision**

Agenda Item: **6.20 (MBMS)**

1 Introduction

Within the 3GPP2 model (and as a candidate key distribution solution for 3GPP) the BAK-keys are securely maintained on the UICC and may be updated by means of OTA (or other)-mechanism from time to time (e.g. 1 day, one week, some hours). A random challenge RAND which is generated at the BM-SC is used to generate session keys on the UICC such that the BAK needs not to leave the UICC. A RAND-value is received together with the MBMS streaming data and allows the mobiles to query the UICC for session keys to be able to decrypt the streaming data. The session keys that are received from the UICC provide confidentiality protection and may optionally provide integrity protection of the streaming data.

Within section 2 it is described how an attacker can take advantage of the fact that the RAND-values in the stream are not protected against replay and that no source authentication is provided. This may allow an attacker to insert malicious content and may lead to MBMS overbilling problems. Subsequently (section 3) an attempt to provide a solution is included. Finally it is proposed to add a new requirement to the TS 33.246.

2 A need to validate RAND freshness at the UICC ?

The current RAND-mechanism does not provide any means for the receivers (i.e. UICC inserted within the mobile) to check if the RAND is fresh. As a consequence the mechanism is vulnerable to RAND-replay and RAND-generation attacks whereby malicious mobile and malicious MBMS source work together.

An example scenario is following: The owner of the malicious mobile subscribes to the service and obtains the BAK key installed on his UICC in a regular way. The malicious mobile does not see the BAK key value (and he does not need to have it for the attack), but is able to intercept all (RAND, SK)-pairs. These (RAND,SK)-pairs are enough to modify, create any arbitrary content and broadcast/multicast this to other mobiles using false RNCs[1] and false BTS thereby making use of some known (or yet unknown) network vulnerabilities. Moreover one (RAND,SK)-pair is enough. The malicious multicast source could then use this pair to behave as the genuine content source and multicast any protected streaming data. Frequent BAK-updating seems to be the only measure to counteract the above threat if the RAND-mechanism is not changed to provide a guarantee of RAND-freshness. Especially if an MBMS service is a concatenation of active and silent sessions (see annex A) then the attacker could first set-up an information gathering phase, initialize the equipment after the first session stop and then take over the MBMS service. But it even does not need to be that difficult. As soon as the BAK-value has been installed on the UICC, the malicious mobile could start querying the UICC to provide him many (RAND, SK)-pairs for use with any arbitrary source that may be transmitted by a malicious MBMS source at any time during the active MBMS session or even before the MBMS session was planned to be started.

[1] A MBMS user in MBMS shall be able to receive MBMS content in idle mode, which means that he need not be connected to the radio network via an authenticated point to point connection.

The risks that such an attack will happen, will increase with the potential customer base that an MBMS service has, as an attacker may like to spread his content to as many users as possible. Concentration of users to particular event (e.g. football station) looks like an ideal target (E.g. they subscribed to a streaming service to receive the goals of the other matches at that moment). Also the confidence in (more-valued) UICC-based MBMS-services could suffer if such an attack happens.

Contribution S3-030529 (SA3#30) proposed[2] to realize an SK-counting function at the UICC. This would then be used to have a usage-based billing mechanism for MBMS at a level of finer granularity than the BAK subscription periods allows. But when RAND values could be replayed by a malicious source then this allows a easy mechanism to create a case of potential overbilling i.e. an 'MBMS overbilling problem' (which only happens if the UICC or terminal collects the billing data).

Siemens believes that solutions to the above described problems are especially justified for MBMS key management solutions based on UICC-mechanism under the assumption that the mechanisms to counteract the threats are NOT more expensive that the cost for an attacker to break his own card to retrieve the key BAK from it.

3 Possible solutions

SOL-1. Change the BAK-key very frequently.

This seems not acceptable due to two reasons:

a) Performing frequent OTA updates seems to make the RAND-concept equivalent to point to point keying concepts in terms of messaging overhead. Furthermore it has already been indicated that OTA should not be used for urgent and frequent updates (See S3-030583: SA3#30).

b) This will not solve overbilling problem if a UICC based SK-counting function would be realized.

SOL-2. Provide a mechanism for RAND freshness.

This requires that a freshness checking mechanism is implemented on the USIM. The USIM shall only deliver the MBMS session keys to the UE if the RAND is deemed to be fresh. A solution seems possible whereby an integrity key is maintained and updated to the UICC similar as the BAK. This integrity key shall protect a sequence number SEQ and number RAND from tampering with during transport. A keyed-hash function with as input the integrity key and SEQ/RAND will add a MAC value to RAND and SEQ. The mobile will then receive SEQ, RAND and MAC, pass all to the UICC which will check MAC validity as well as check if SEQ is not old and will only give back session keys to the mobile if the SK-generation data gets through the validation steps.

Other alternative solutions may be possible.

4 Proposed new requirement for TS 33.246

The base requirement text was taken from section 4.1.1 in S3-030517 v0.2.1 (SA3#30)

[2] But was not yet agreed

4.1.1 Requirements on MBMS Key Management

R5a: The transfer of the MBMS keys between the MBMS key generator and the UE shall be confidentiality protected.

R5b: The transfer of the MBMS keys between the MBMS key generator and the UE may be integrity protected.

R5c: The UE and MBMS key generator shall support re-keying to ensure that users that have joined a multicast service, but then left, shall not gain further access to the multicast service without being charged appropriately. The re-keying shall also ensure that users joining a multicast service shall not gain access to data from previous transmissions in the multicast service without having been charged appropriately

R5d: Only authorized users that have joined an MBMS multicast service shall be able to receive MBMS keys delivered from the MBMS key generator.

R5e: The MBMS key encryption key shall not allow the BM-SC to infer any information about used UE-keys at radio level (i.e. if they would be derived from it).

R5f: A UICC, realizing the function of providing session keys for decrypting the streaming data at the UE, shall only give session keys back to the UE if the input values used for obtaining the session keys were fresh (have not been replayed) and came from a trusted source.

5 Conclusion

Siemens proposes to **add the requirement R5f**, as listed in Section 4 of this contribution, to the MBMS specification. Solutions for this requirement may be elaborated and its feasibility be decided at SA3#32.

Siemens proposes to adopt the principle that '**Solutions to provide *'source authentication of key generation material received at the UICC'* and *'freshness of key generation material received at the UICC'* shall be available before UICC-based usage-billing solutions can be adopted'**. Otherwise this would open the possibility for potential MBMS overbilling attacks.

Annex A: Phased Streaming Sessions (TS 23.246)

Following timeline has been copied from TS 23.246v600 and is for information only :

The phases subscription, joining and leaving are performed individually per user. The other phases are performed for a service, i.e. for all users interested in the related service. The sequence of phases may repeat, e.g. depending on the need to transfer data. Also subscription, joining, leaving, service announcement as well as MBMS notification may run in parallel to other phases.

This is illustrated with the following example of timeline:

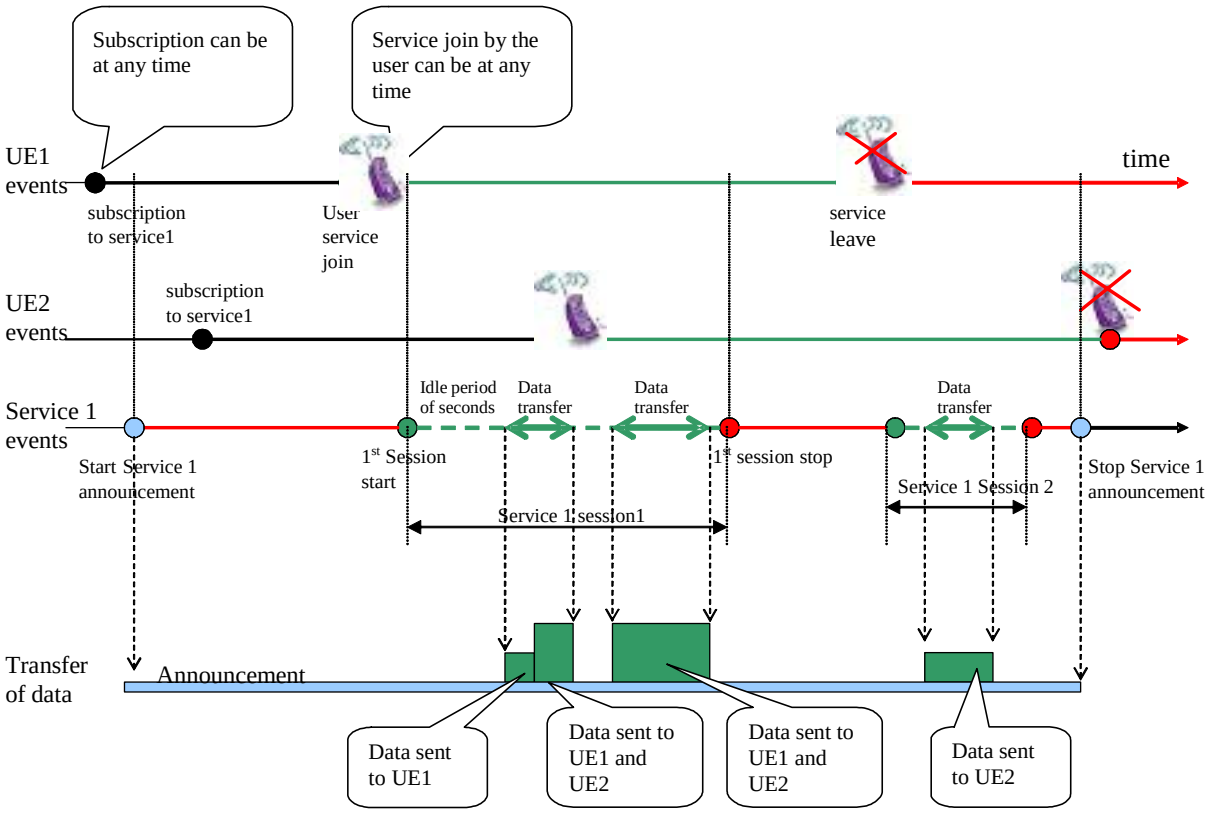

Figure 3: Timeline example