3GPP TSG SA WG3 Security — S3#26 **S3-020635**

19 - 22 November 2002

Oxford, UK

Source: **Siemens**

Title: **Integrity protection for MBMS data**

Document for: **Discussion and Decision**

Agenda Item: **7.19**

Abstract

This contribution discusses integrity protection requirements of MBMS user data. When it is assumed that MBMS users cannot be trusted then using shared keys (integrity and confidentiality) among a group of users can only prevent attacks of lower levels of sophistication, such as prevent eavesdroppers from simply listening in. For closed MBMS- user groups (i.e. railways), where it can be assumed that users can be trusted, using integrity protection can provide protection against outsider attacks.

1) Status of the discussion at SA3#25

SA3#25 in Munich discussed shortly the requirement on integrity protection (R3a to R3c) as available now in [S3-020604]. During the discussions, there were given some arguments against the usefulness of integrity protection on the MBMS data, but it was also argumented that it should be impossible for an intruder to insert or modify MBMS data packets in a meaningfull way such that the MBMS user would be misled. The scenario example given, was a speech of President Bush where an attacker was able to change essential parts of his speech.

This contribution looks at the scope of the requirement and the usefulness of integrity protection in order to make a final decision on this requirement.

2) Comments on current MBMS multicast data integrity protection requirements.

The requirements as postulated by [S3-020604] and original provided by [S3-020532] are:

R3a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS multicast data sent to the UE on the radio interface.

Editor's note: Requirement R3a has not been agreed.

R3b: The MBMS multicast data may be integrity protected with a common integrity key, which shall be available to all users that has joined the MBMS service.

R3c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi and Gmb.

Editor's Note: It may be required to integrity protect the multimedia content on the "Content Provider - BM-SC" interface. As this interface shall not be standardized in 3GPP, according to TR 23.846, no such requirement can be defined by 3GPP.

Comments:

1) The requirements for integrity protection in [S3-020604] have been restricted to apply to multicast data only. But as 'data authentication necessity' is independent from the way it is distributed to the user, there is no reason why multicast data should be integrity protected and broadcast data not. It may be that the same content will be broadcasted in one area (accompanied by advertisements) while in another operators area this is multicasted (and the users have to pay for it). The stage 1 MBMS specification [MBMS Stage 1] makes only a distiction between broadcast and multicast mode due to charging requirement, and not due to data sensitivety.

2) The Gmb reference point between BM-SC and GGSN enables the BM-SC to exchange MBMS service control information with the GGSN. It does not transfer MBMS multicast data but signalling data. R3c specifies optional protection of Gmb. When not providing integrity protection on Gmb, then an attacker will be able to control the service on GGSN. Integrity protection on Gmb shall be mandated and it is therefore proposed to separate the requirements of the Gmb and Gi-interface from eachother.

   Proposed requirement: 'The Gmb interface shall be integrity protected'.

   When these service control messages run on top of an IP-stack, than NDS/IP methods could be used to provide integrity protection. This requirement does not belong to Clause 4.1.2 but should be included in a separate clause.

3) Discussion on the need for integrity protection

3.1 Assumptions

Assumptions on location of MBMS-components and trust relations - (in accordance with [MBMS stage 1]):

- The content provider may be located outside the operators network.
- The BM-SC is located within the operators network and is the connection point of the content provider with the operator. (The case where a content provider [MBMS stage 2 configuration figure 1] is connected directly to the GGSN is not analysed here, as the BM-SC is not in the path between the UE and the content provider)
- The BM-SC is connected with the content provider receiving the MBMS data via unicast or multicast.

Further assumption:

- Integrity protection is based on a shared key between the MBMS-source and the MBMS users (a secret key used in a symmetric algorithm as described in R3b).

3.2 MBMS users cannot be trusted.

The assumption that MBMS users can not be trusted, will be applicable in open MBMS groups (i.e. UMTS, GSM users).

Following facts seems to weaken the usefulness of integrity protection on the path from the BM-SC to the UE.

1) An integrity key that is shared by many MBMS user and the MBMS multicast source, does not allow to authenticate the multicast source. Any of the MBMS users could fake the MBMS multicast source (so be able to insert MBMS data in the network)

2) An attacker who is so sophisticated as to modify encrypted data on a communication interface may also be assumed to be able to retrieve keys from his UE.

3) It will also be equally difficult or easy to retrieve an encryption or integrity key from a UE. Consequentially it can be assumed that if an attacker possesses valid MBMS keys, he will have both.

A scenario similar (initiated from an untrusted insider, or outsider cooperating with untrusted insider) as those mentioned in [S3-020504] may be applied to initiate data modification: A malicious user retrieves both Integrity and Confidentiality key from the UE, whereafter the keys are used to insert/replace MBMS data in the network or radio path between source and destination. Also the same techniques that were presented for the encryption key in [S3-020504] can also be applied here, but it can never give a 100% guarantee that the data of the content provider did reach all intended UE's in an unmodified way. The user will not even know, as the integrity check may not have failed.

The conclusion is here that using shared keys (integrity and confidentiality) among a group of users can only prevent attacks of lower levels of sophistication, such as prevent eavesdroppers from simply listening in.

3.3 MBMS users can be trusted.

The assumption that MBMS users can be trusted, may be applicable in closed MBMS users groups (i.e. railways usage).

None of the arguments from the previous clause hold now and including integrity protection can indeed be useful against outsider attacks. Attack scenarios from an outsider such as data deletion, modification and data insertion will be detected at the MBMS user side.

4) Conclusion

This contribution tried to clarify the integrity protection requirements. When it is assumed that MBMS users cannot be trusted then using shared keys (integrity and confidentiality) among a group of users can only prevent attacks of lower levels of sophistication, such as prevent eavesdroppers from simply listening in. For closed MBMS- user groups (i.e. railways), where it can be assumed that users can be trusted, using integrity protection can provide additional protection against outsiders.

5) References

[S3-020504]: MBMS - Fraud and countermeasures (Siemens), SA3#25 Munich, Germany, Oct 2002

[S3-020532]: MBMS – Trust and Threats (Ericsson), SA3#25 Munich, Germany, Oct 2002

[MBMS Stage 1]: 3GPP TS 22.146 V5.2.0 MBMS stage 1 (2002-3).

[S3-020604]: 3GPP TS 33.cde V0.0.2 Security of Multimedia Broadcast/Multicast Data (2002-11)