3GPP TSG SA WG3 Security **S3-020532**

October 9-12, 2002

Munich, Germany

Agenda Item: MBMS

Source: Ericsson

Title: 7.19 MBMS – Trust and Threats

Document for: Discussion and decision

1. Introduction

This contribution shows the MBMS architecture, describing the roles and their trust relationships. This document also describes some potential threats and attacks. The purpose is to help 3GPP identify security requirements for the MBMS system, and choose suitable security mechanisms fulfilling those requirements.

1.1 MBMS network architecture

SA2 is currently working on the MBMS architecture and has just finalised a technical report in TR 23.846, which was agreed at SA plenary # 17. The following picture captures the current MBMS architecture that SA2 is working on:

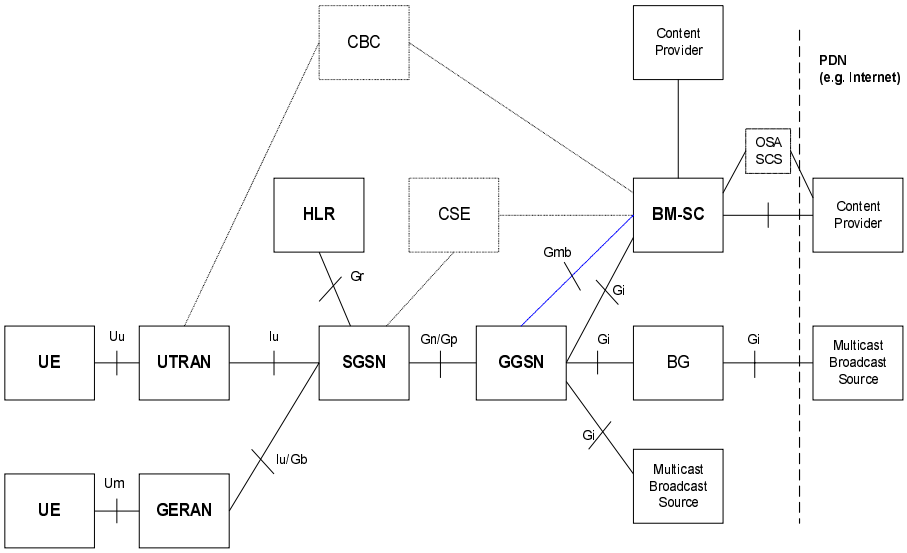

Figure 1:

This paper is considering the following network entites:

SGSN: In the MBMS architecture the SGSN performs user individual service control functions and the SGSN concentrates all individual users of the same MBMS service into a single MBMS service. The SGSN maintains a single connection with the source of the MBMS data.

GGSN: The GGSN terminates the MBMS GTP tunnels from the SGSN and links these tunnels via IP multicast with the MBMS data source.

BM-SC: The BM-SC is an MBMS data source. MBMS data may be scheduled in the BM-SC, e.g. for transmission to the user every hour. It offers interfaces over that content provider can request data delivery to users. The BM-SC may authorise and charge content provider.

Content provider: A Content Provider provides the 3GPP network with multimedia content (as text, audio, picture, video). According to TR 23.846 the reference point from the content provider to the BM-SC is not standardised. The content provider could be an external entity to the 3GPP network.

1.2 MBMS service availability

It can be useful to mention the requirements in SA1 regarding MBMS service availability.

A PLMN operator shall be able to provide service announcements for a multicast service within and outside of the multicast area defined for the multicast service. Although the user/subscriber is aware of multicast services by announcements that are not available at the current location, the user/subscriber can not join them until the user/subscriber is in the multicast area where they are available.

A multicast area may cover (parts of) one or more PLMN's.

For joining and activation of a MBMS multicast service, the following requirements can be useful to mention:

- The end-user/subscriber can join/activate a local MBMS service in a HPLMN.
- The end-user/subscriber can join/activate a local MBMS service in a VPLMN, if the user's home environment allows it.
- While the user/subscriber is roaming in a VPLMN, the user/subscriber can join/activate a MBMS multicast service in his HPLMN, if the multicast service in the HPLMN covers the VPLMN as well and the MBMS multicast service in the HPLMN is announced in the VPLMN to the user/subscriber.
- The user/subscriber can join/activate a local MBMS service in HPLMN and then roam into a VPLMN and still gain access to the MBMS service from the HPLMN.
- The user/subscriber can join/activate a local MBMS service in VPLMN-1, if the user's home environment allows it and then roam into another VPLMN-2 and still gain access to the MBMS service from the VPLMN-1.

1.3 Roles

For the purposes of security analysis, the following roles are identified:

- Home network
- Serving network
- User/subscriber
- Content Provider, external or internal to the 3GPP network operator

1.4 Assets

1.4.1 Network access

1.4.1.1 3GPP operator charges user

The SGSN generates charging data per MBMS multicast service for each user. This charging information may include duration of a complete MBMS multicast session, volume of MBMS multicast data, time when joining and leaving a multicast group.

The business model of public access hinges on the operator's ability to correctly charge the user for network access for MBMS multicast service.

It seems though like the system can't assure that the MBMS multicast data has been delivered successfully to the user. This would require acknowledgements from the UE's, which does not seem practical, as it would overload the network.

Three different charging models are discussed in SA1:

Multicast session duration:

The operator charge the user based on a whole multicast session.

If the user leaves the multicast session before the session has ended, the user will still be charged for the whole session. It does not matter to the user if someone else is using his identity after he left, to gain access to the multicast session. From the operator view this can be seen as a lost customer.

In case of any active attack on the multicast data or transmission error of the multicast data, the user will be charged for the whole multicast session.

MBMB data volume-based charging

The user could pay for the number of bytes transferred to the device.

In this charging model someone else could use the user's identity to gain access to the multicast service, but the real user would still be charged.

In case of any active attack on the multicast data or transmission error of the multicast data, the user would be charged anyway for the transferred bytes.

Time when joining and leaving a multicast subscription group or multicast group, duration of membership to a multicast group

The user is charged when joining and leaving a group i.e. charging is based on the time duration of have joined a MBMS multicast service.

In this charging model someone else could use the user's identity to gain access to the multicast service, and the real user would still be charged.

In case of any active attack on the multicast data or transmission error of the multicast data, the user will be charged anyway.

1.4.1.1 Content Provider charges 3GPP operator

The Content Provider will most likely charge the 3GPP network for the provided multimedia content.

1.4.2 3GPP operator network

From the operator's perspective, it is important that the security level provided for MBMS multicast data is the same as for any other 3G services offered by the 3GPP operator to the users today.

It's in the interest of the 3GPP operator to secure the multimedia content provided by the content providers on the BM-SC <-> Content Provider interface, as the 3GPP network most likely will be charged by the content provider.

1.4.3 Content provider

The Content Provider will most likely charge the 3GPP network for the provided multimedia content.

1.4.4 User/subscriber

For the MBMS user it's important that no one else can access the 3GPP network by using the user's identity to gain "free access" of MBMS services on the user's bill.

The MBMS user does not want to get charged for MBMS multicast data that has been attacked or encountered transmission errors.

1.5 Trust relation ships

The following trust relationship between the roles that are participating in MBMS services are proposed:

The user trusts the home network operator to provide the MBMS service according to the service level agreement. .

The home operator trusts the user to be accountable for his actions.

The user trusts the network operator after mutual authentication.

The network trusts an authenticated user using integrity protection and encryption at RAN level.

The network may have trust or no trust in a content provider.

The home network and visited network trust each other when a roaming agreement is defined, in the case the user is roaming in a VPLMN.

1.6 Threats associated with attacks on the radio interface

The threats associated with attacks on the radio interface are split into the following categories, which are described in the following sub-chapters:

- unauthorized access to multicast data;
- threats to integrity;
- denial of service;
- unauthorized access to MBMS services;
- privacy violation;

The attacks on the MBMS service announcements to the users on the radio interface are not discussed here, as these will most likely be transferred on a point-to-point connection (e.g. PS signaling connection), which is already secured today (integrity protected and optionally encrypted RAN level).

1.6.1 Unauthorised access to multicast data

- A1: Intruders may eavesdrop MBMS multicast data on the air-interface.
- A2: Users that have not joined and activated a MBMS multicast service shall not be able to gain a MBMS multicast service without being charged.
- A3: Users that have joined and then left a MBMS multicast service shall not be able to continuing receiving the MBMS multicast service without being charged.

1.6.2 Threats to integrity

- B1: Modifications and replay of messages in a way to fool the user of the content from the actual source, e.g. replace the actual content with a fake one.

1.6.3 Denial of service attacks

- C1: Jamming of radio resources. Deliberated manipulation of the data to disturb the communication.

1.6.4 Unauthorised access to MBMS services

- D1: The MBMS user must be sure that no one else can access the 3GPP network to gain “free access” of MBMS services and other services on the user’s bill.

1.6.5 Privacy violation

- E1: The user identity could be exposed to the content provider, in the case the content provider is located in the 3GPP network, and then linked to the content.

1.7 Threats associated with attacks on other parts of the system

The threats associated with attacks on other parts of the system are split into the following categories, which are described in the following sub-chapters:

- unauthorized access to data;
- threats to integrity;
- denial of service;

1.7.1 Unauthorised access to data

- **F1**: It is assumed that the BM-SC and the GGSN are located in the same network. The BM-SC can though be located in a different place than the GGSN, and therefore can open up for intruders who may eavesdrop the new interface Gi and Gmb between the BM-SC and GGSN.
- **F2**: Intruders may eavesdrop the new interface between the content provider and the BM-SC.

1.7.2 Threats to integrity

- **G1**: It is assumed that the BM-SC and the GGSN are located in the same network. The BM-SC can though be located in a different place than the GGSN, and therefore can open up for new attacks on the new interfaces Gi and Gmb between the BM-SC and GGSN.
- **G2:** The new interface between the content provider and the BM-SC may open up for attacks as modifications of multimedia content.

1.7.3 Denial of service

- **H1**: Deliberated manipulation of the data between the BM-SC <-> Content Provider to disturb the communication.
- **H2**: Deliberated manipulation of the data between the BM-SC <-> GGSN to disturb the communication.

1.8 Security Requirements

1.8.1 Requirements on security service access

1.8.1.1 Requirements on secure service access

- R1a: A valid USIM shall be required to access any 3G service including the MBMS service.
- R1b: It shall be possible to prevent intruders from obtaining unauthorized access of MBMS services by masquerading as authorized users.

1.8.1.2 Requirements on secure service provision

- R2a: It shall be possible for service providers (i.e. BM-SC) to authenticate users at the start of, and during, service delivery to prevent intruders from obtaining unauthorized access to MBMS services.
- R2b: It shall be possible to prevent the use of a particular USIM to access MBMS services.

[Editor's Note: It is for FFS to what extent it is required to detect and prevent fraudulent use of MBMS services.]

1.8.2 Requirements on integrity protection of MBMS multicast data and security keys

- 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.
- 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.
- R3d: 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.]

1.8.3 Requirements on encryption protection of MBMS multicast data and security keys

- R4a: It shall be possible to protect the confidentiality of MBMS multicast data on the radio interface.
- R4b: The MBMS multicast data may be encrypted with a common encryption key, which shall be available to all users that has joined the MBMS service.
- R4c: The encryption key(s) and the integrity key for the MBMS multicast service shall be encrypted when delivered to the users. In addition, it may be required to protect these keys with a MAC.
- R4d: Only the valid users that has joined a MBMS multicast service shall be able to decrypt the encryption key(s) and the integrity key delivered from the network.
- R4e: Mandate support of re-keying in the UE and BM-SC in order to ensure that users that has joined a MBMS service, but then left, shall not gain MBMS multicast service without being charged.
- R4g: It may be required to encrypt the MBMS multicast data on the "BM-SC - GGSN" interface, i.e. the reference points Gi and Gmb.
- R4h: User identity should not be exposed to the content provider or linked to the content, in the case the Content Provider is located in the 3GPP operator's network.

[Editor's Note: It may be required to encrypt 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.]

1.9 Conclusion

This paper proposes to that SA3 discusses and adopts the security requirements in chapter 1.8.