CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ 33.246 CR ⌘rev - ⌘ Current version: 1.1.0 ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	Additions to threats section (Annex B)
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	29/03/2004
Category:	⌘	
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Adding the threats that lead to the introduction of MTK key replay protection and MTK Key freshness checks (See contribution S3-030701)
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	Annex B

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	-

**********First change **********

Annex B (informative): Security threats

This annex contains some security threats that have been identified for MBMS.

B.1 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).

B.1.1 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 receiving that service without being charged.

A3: Users that have joined and then left a MBMS multicast service continuing to receive the MBMS multicast service without being charged.

A4: Valid subscribers may derive decryption keys (MTK) and distribute them to unauthorized parties.

Note: It is assumed that the legitimate end user has a motivation to defeat the system and distribute the shared keys (MSK, MTK) that are a necessary feature of any broadcast security scheme.

B.1.2 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.

B.1.3 Denial of service attacks

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

B.1.4 Unauthorised access to MBMS services

D1: An attacker using the 3GPP network to gain "free access" of MBMS services and other services on another user's bill.

D2: An attacker using MBMS shared keys (MSK, MTK) to gain free access to content without any knowledge of the service provider.

Note: It cannot be assumed that keys held in a terminal are secure. No matter how the shared keys (MSK, MTK) are delivered to the terminal, we have to assume they can be derived in an attack. For example, the shared keys, while secure in the UICC, may be passed over an insecure SIM-ME interface.

B.1.5 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.

B.2 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;

A malicious UE generating MTKs for malicious use lateron.

Unauthorized insertion of MBMS user data and key management data.

B.2.1 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.

B.2.2 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.

B.2.3 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.

B.2.4 A malicious UE generating MTKs for malicious use lateron.

K1: A malicious ME querying the MTK generation function for MTK's to use them lateron in an attack (e.g. in order to use the retrieved MTK's within unauthorized data insertion attacks (See B.2.5)).

B.2.5 Unauthorised insertion of MBMS user data and key management data

J1: An ME which deliberately inserts key mananagement and malicious data, encrypted with valid (previously retrieved) MTK from the MTK generation function, within the multicast stream.

J2: An ME which deliberately inserts key management and malicious data, encrypted with old (using replayed key management messages) MTK, within the multicast stream