3GPP TSG SA WG3 Security — S3#34 **S3-040553**

July 6 - 9, 2004

Acapulco, Mexico

Title: **Source Origin Authentication in MBMS**

Source: **Ericsson**

Document for: **Discussion and decision**

Agenda Item:

Work Item: **MBMS**

1 Introduction

In SA3#33 Ericsson presented a contribution [1] on integrity protection and source origin authentication (SOA). The meeting felt that more analysis is needed on the threats involved. The current contribution discusses the threats that SOA could mitigate and provides the status of a mechanism that could provide SOA.

2 Discussion

2.1 Threats that would require SOA

As was noted in [1] applications that would require integrity protection/ SOA include e.g. distribution of stock market quotes and public emergency messages. Lack of integrity protection/ SOA in these applications could be catastrophic if users can be tricked to make severely incorrect decisions based on the multicast information. It is noted that integrity protection alone only restricts the possible attacker outside the multicast group as any group member having the group key (i.e. MSK) could forge messages coming from the BM-SC. However, multicast services may have wide audience and therefore be a tempting target for attacks. Any extra security, even if not 100% proof, makes the system less vulnerable to attacks.

A specific attack in MBMS is where an attacker that does not posses the MSK sends multicast packets (either data packets or MTK delivery packets) with fake key identifiers (i.e. MSK identifier) in the multicast stream. This will launch a DOS attack towards the BM-SC since UEs will not recognize the MSK identifier and thus will request for a new MSK. It should be noted that integrity protection does not help in this situation even against attackers from outside the group, since the integrity protection of the multicast packets is based on MSK and MSK is the key the UE thinks he is missing. This use case is of specific importance because UEs should have a way to retrieve the current MSK when they detect from the traffic or MTK delivery messages that they are missing it. This is indicated in requirement R5f in TS 33.246 [2]:

> *R5f: All keys used for the MBMS User Service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.*

A companying pseudo CR introduces the new threat and corresponding requirement to mitigate the threat in TS 33.246.

2.2 Status of TESLA

A mechanism to implement source origin authentication is TESLA (Timed Efficient Stream Loss-tolerant Authentication protocol). The progress of TESLA in IETF is currently rather slow. The TESLA specification [3] is currently obsolete in IETF since internet drafts have a six month expiry time, but it still is in IETF internet draft tracking list (in state "AD is watching"). The TESLA introduction [4] is in state "AD evaluation". They are not expected to be ready in Rel-6 time frame, but if they are put in 3GPP – IETF dependency list, their development could be enhanced.

It should be noted that some concerns raised against TESLA during previous SA3 meetings are not that strong. For instance it has been claimed that TESLA requires public key cryptography. While it is true that the "anchor" of the hash-chain needs to be delivered over an authenticated channel, we already have such a channel in MBMS in form of MUK-protected delivery (point-to-point from the BM-SC to each UE). There is no need to use signatures in this case. Moreover, it was claimed that TESLA is complex. It seems very unlikely that a much less complex scheme for SOA based on symmetric key cryptography will be available in a reasonable time frame.

3 Conclusions and proposal

Threats involved due to lack of integrity protection and SOA should be studied further. At least attack on key identifiers seems to be one threat requiring SOA. A companying pseudo CR introduces this threat and corresponding requirement in TS 33.246.

In the meantime, it should be ensured that SOA is a possible way forward in the future releases. It should be noted that work is under way to add SOA support in SRTP [5].

4 References

[1] TD S3-040230, On the need for integrity and source origin authentication in MBMS, Ericsson, SA3#33

[2] 3GPP TS 33.246 v 1.2.1, MBMS Security

[3] IETF, draft-ietf-msec-tesla-spec-01.txt, Internet Draft,

[4] IETF, draft-ietf-msec-tesla-intro-02.txt, Internet Draft, May 2004

[5] IETF, draft-ietf-msec-srtp-tesla-00.txt, Internet Draft, February 2004

3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040553_Att1

CR-Form-v7

CHANGE REQUEST

⌘	**33.246**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**1.2.1**	⌘

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:	⌘	Key identifier attack in MBMS		
Source:	⌘	Ericsson		
Work item code:	⌘	MBMS	***Date:*** ⌘	29/06/2004
Category:	⌘	**B**	***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:	⌘	In the current TS 33.246 it is specified that the UE should be able to retrieve the actual key (i.e. MSK) based on identity match, and mismatch recognition when an MSK update was missed or was erroneous/incomplete. However, this possibility opens up a new threat, since an attacker that does not posses the MSK can insert multicast packets (data packets or MTK delivery packets) in the multicast stream and launch a DOS attack against the BM-SC. It should be noted that this attack could be launched even outside the group and is not mitigated with integrity protection since integrity protection is based on MSK.
Summary of change:	⌘	The threat is added to the threat section. A corresponding requirement is added to the requirement section.
Consequences if not approved:	⌘	A DOS attack against the BM-SC is possible.

Clauses affected:	⌘	B.2.5, C.4, C.5				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

*********************************** NEXT CHANGE ********************************

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

J3: An attacker, which deliberately inserts packets with fake Key-ID (or modifies the Key-ID of packets) within the multicast stream may cause Denial of Service attack if all or many of the UEs request for the MSK that was indicated in the fake Key- ID.

*********************************** NEXT CHANGE ********************************

C.4 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 the operator to perform re-keying as frequently as it believes necessary to ensure that

- users that have joined an MBMS User Service multicast service, but then left, shall not gain further access to the MBMS User Service without being charged appropriately
- users joining an MBMS User Service shall not gain access to data from previous transmissions in the MBMS User Service without having been charged appropriately
- the effect of subscribed users distributing decryption keys to non-subscribed users shall be controllable.

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

R5e: The MBMS keys 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: All keys used for the MBMS User Service shall be uniquely identifiable. The identity may be used by the UE to retrieve the actual key (based on identity match, and mismatch recognition) when an update was missed or was erroneous/incomplete.

Editor's note: If ptm re- keying is used, the keys shall be delivered in a reliable way. Ptp re-keying is assumed to be reliable.

R5g: The BM-SC shall be aware of where all MBMS specific keys are stored in the UE (i.e. ME or UICC).

R5h: The function of providing MTK to the ME shall only deliver a MTK to the ME if the input values used for obtaining the MTK were fresh (have not been replayed) and came from a trusted source.

R5i: ADOS attack should be mitigated where an attacker that does not possess the MSK inserts multicast packets (data packets or MTK delivery packets) with fake Key-ID (or modifying Key-IDs of packets) in the multicast stream and causes all or many UEs to request for a MSK from the BM-SC.

C.5 Requirements on integrity protection of MBMS User Service data

R6a: It shall be possible to protect against unauthorized modification, insertion, replay or deletion of MBMS User Service data sent to the UE on the radio interface by an attacker that does not possess the MSK. The use of integrity shall be optional.

Editor's note: It may be possible to detect the deletion of MBMS data packets, but it is impossible to prevent the deletion. Packets may be lost because of bad radio conditions, providing integrity protection will not help to detect or recover from this situation.

Note: the use of shared keys (integrity and confidentiality) to a group of untrusted users only prevents attacks of lower levels of sophistication, such as preventing eavesdroppers from simply listening in

R6b: The MBMS User Service data may be integrity protected with a common integrity key, which shall be available to all users that have joined the MBMS User Service.

R6c: It may be required to integrity protect the "BM-SC - GGSN" interface i.e. reference point Gi.