3GPP TSG SA WG3 Security — S3#36 **S3-040992**
23 – 26 November 2004
Shenzhen, China

Source: **Ericsson, TeliaSonera**

Title: **The need for and use of salt in MBMS streaming (Updated)**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

1 Introduction

This paper is an update of S3-040796 and discusses the use of salt as a countermeasure to pre-computation attacks against the MBMS streaming system.

Security is not an easy subject, and it takes long time to develop a solution that most people feel comfortable with. This is the case with the salt in SRTP. The SRTP draft would not have been accepted as an RFC in IETF if the salt had been left out.

It is our belief that the question should not be whether the salt is needed, but rather if it is safe to remove it. Note that the salt usage is a part SRTP, and it was included for a reason (which is explained in Section 2).

2 The need for salt

A salt is some random bits that are incorporated in a cryptographic process, e.g. encryption, key derivation, etc, and cannot be predicted before the process begins. The salt does not need to be secret; the important thing is that it is completely unknown before the process begins.

For encryption, the purpose of the salt is to protect against key collision attacks, which basically works as follows:

- The attacker guesses (or knows) some portion of plaintext that will later be encrypted. This is reasonable to assume, most protocols include fields that are known or easily guessable [1].
- He then encrypts this plaintext under a number of distinct keys, and stores the (cipher-text, key)-tuple in a database.
- The attacker records encrypted traffic from the streaming source (which changes the encryption key from time to time) and looks for a cipher-text that collides with one he has in his database.
- If a collision is found, he can look up which key he used to produce that cipher text.

Of course there may sometimes be one or more cipher texts in the database that matches, but the number is usually small enough that a brute force search is feasible.

More advanced key collision attacks against stream ciphers do not require known plain-text, but only linear relations between bits in the plain-text, [1]. This *will* be present in the MBMS streams since we are to encrypt codec data etc., and especially if normal FEC is used.

The effective key length is reduced from *n* bits down to *n – log(M)*, where *M* is the number of distinct keys the attacker has in his database.

Two things can be noted. First, the attack works against *any* stream cipher, and secondly, the more frequent the re-keyings are, the faster the attacker will find a collision.

The salt, which is used to "extend" the effective key length, by preventing the attacker from performing the pre-computation step without also guessing the salt.

For key derivation, similar caveats apply to avoid pre-computation attacks.

3 How the salt is used in the encryption

As is stated in RFC3711 [2], the salt is incorporated in the encryption process by xor:ing it into the IV. In other words, the mechanism for using the salt is already present in SRTP, and all interfaces are in place.

Note that this use of salt also relaxes the assumptions on the block cipher used. Since the salt (which is randomly generated) is xor:ed into the IV, the block cipher only has to be assumed to be good for random IVs, whereas it would have to be good for *all* fixed IVs. The word "good" is to be read in the sense that the output of the block cipher looks random.

4 Transportation of salt

The salt is sent from the BM-SC in the KEMAC payload (which also contains the key) to the UE. It is already specified in MIKEY [3] how the salt is incorporated in the KEMAC payload. MIKEY also provides the possibility to derive the salt from the key in the message, but to provide enough entropy, the delivered MTK would have to be longer if this technique is used.

5 Conclusion and proposal

The use of salt is required in MBMS to not shorten the effective key length, and all mechanisms to use it are already in place in the protocols used. We propose that the accompanying pseudo CR is implemented.

6 References

[1] McGrew and Fluhrer, "Attacks on Additive Encryption of Redundant Plaintext and Implications on Internet Security", http://www.mindspring.com/~dmcgrew/dam.htm
[2] Baugher et. al., "The Secure Real-time Transport Protocol (SRTP)", RFC3711, IETF
[3] Arkko et. al., "Multmedia Internet KEYing (MIKEY)", RFC3830, IETF
[4] Ericsson, "The need for and use of salt in MBMS streaming", S3-040796, 3GPP

3GPP TSG-SA3 Meeting #36 ***Tdoc ⌘Att1_S3-040992***
Shenzhen, China, 23 – 26 November 2004

CR-Form-v7

CHANGE REQUEST

⌘ **33.246** **CR** **010** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

*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⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	MBMS Transport of salt
Source:	⌘	Ericsson, TeliaSonera
Work item code:	⌘	MBMS
Date:	⌘	20/09/2004
Category:	⌘	**C**
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:	⌘	The protection of the MBMS traffic will not meet the commonly required design goal of having a security level equivalent to the key size.
Summary of change:	⌘	The salt needed by SRTP is sent in the KEMAC payload of the MIKEY message containing the MTK. Note that CR S3-040850 is taken into consideration.
Consequences if not approved:	⌘	The protection of the MBMS traffic will be vulnerable to pre-computation attacks.

Clauses affected:	⌘	6.4.6.2, 6.5.4

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

Other comments:	⌘	

__FIRST_CHANGE__

6.4.6.2 MTK MIKEY Message Reception

When the MIKEY message arrives at the ME, the processing proceeds following the steps below (basically following section 5.3 of [9]).

1. The Data Type field of the common MIKEY header (HDR) is examined, and if it indicates an MTSK delivery, the MSK ID is extracted from the Extension Payload.

2. The Timestamp Payload is checked, and the message is discarded if the counter in the Timestamp Payload is ~~larger~~ smaller or equal to the ~~current MIKEY~~stored replay counter associated with the given MSK (the stored replay counter value is retrieved from MGV-S). To avoid issues with wrap around of the ID fields ``smaller than´´ should be in the sense of RFC1982 [10].

3. If the MTK ID extracted from the Extension payload is less than or equal to the current MTK ID (kept in the ME), the message shall be discarded.

4. The message is transported to MGV-F for further processing, cf 6.5.3.

5. The MGV-F replies success (i.e. sending the MTK and possibly salt) or failure.

__SECOND_CHANGE__

6.5.4 MTK validation and derivation

When the MGV-F receives the MIKEY message, it first determines the type of message by reading the Data Type field in the common header. If the key inside the message is an MTK, MGV-F retrieves the MSK with the ID given by the Extension payload.

It is assumed that the MBMS service specific data, MSK and the sequence number SEQs, have been stored within a secure storage (MGV-S). Both MSK and SEQs were transferred to the MGV-S with the execution of the MSK update procedures. The initial value of SEQs is determined by the service provider.

The MGV-F shall only calculate and deliver the MBMS Traffic Keys (MTK) to the ME if the ptm-key information is deemed to be fresh.

The MGV-F shall compare the received SEQp, i.e. MTK ID from the MIKEY message with the stored SEQs. If SEQp is equal or lower than SEQs then the MGV-F shall indicate a failure to the ME. If SEQp is greater than SEQs then the MGV-F shall calculate the MAC as defined in [9] using the received MIKEY message and MSK as input. This MAC is compared with the MAC of the KEMAC payload in the MIKEY message. If the MAC verification is unsuccessful, then the MGV-F will indicate a failure to the ME. If the MAC verification is successful, then the MGV-F shall update SEQs with SEQp value and start the generation of MTK. The MGV-F provides the MTK to the ME.

If MAC verification is successful, ~~T~~the MGV-F shall update in MGV-S the counter value in the Time Stamp payload associated with the corresponding MSK ID.

In the case of streaming, SRTP requires a master key and a master salt. The MTK is used as master key, and the salt in the KEMAC payload is used as master salt.

NOTE: MIKEY includes functionality to derive further keys from MTK if needed by the security protocol. The key derivation is defined in section 4.1.3 of MIKEY [9].