3GPP TSG SA WG3 Security — S3#35 **S3-040792**
5 - 8 October 2004
Malta

Source: **Ericsson**

Title: **MBMS Key derivation chain**

Document for: **Discussion and decision**

Agenda Item: **MBMS**

1 Introduction

This paper describes how the key derivation chain (induced by the three level key hierarchy in MBMS) can be achieved with the use of MIKEY [1]. It is basically a description of how MIKEY works, and shows how to plug in MBMS-specific values in the parameters. There are no new functionalities introduced that are not already present in MIKEY.

2 MIKEY Background

This section gives some background on the internal MIKEY functionality.

MIKEY [1] specifies a pseudo random function (PRF) that is used to generate cryptographically independent keys from its inputs. This PRF has been scrutinized (and accepted) by the IETF, and is very similar to the PRF used in TLS [2]. The PRF serves two purposes in the protocol:

- Deriving keys from the pre-shared secret that are used internally in the MIKEY protocol to protect the KEMAC payload,
- and to derive several keys for the security protocol from a single exchanged key.

A TEK (transport encryption key) is in MIKEY terminology the key that is sent directly to the security protocol, and a TGK (TEK Generation Key) is the key from which the TEK is derived.

To protect the KEMAC payload, MIKEY derives a confidentiality-, an integrity- and a salting key. These keys are used internally in the MIKEY protocol. The inputs to the PRF in this case are the pre-shared key, Crypto Session ID, RAND and a constant that determines which type of key is to be derived.

The inputs to the PRF when generating keys for a security protocol from a TGK are: The TGK itself, Crypto Session ID, Crypto Session Bundle ID, RAND and a constant that is different depending on which type of key is to be derived (confidentiality key, integrity key, salting key or TEK). The TEK can be used when the security protocol itself further derives separate integrity, confidentiality and salting keys. If the security protocol cannot do it on its own, MIKEY can do the derivation on behalf of the protocol.

3 MSK delivery and MUK derivation

In this section it is assumed that the MUK is installed in the UE. The MUK is used as a pre-shared key in the MIKEY protocol. When the P2P message containing an MSK reaches the UE, the UE runs MIKEY with the MUK as pre-shared key. This results in that MIKEY internally runs the PRF to derive MUK_C, MUK_I and MUK_S as follows:

- MUK_C = PRF(MUK, ”encryption key constant” | 0xFF | CSB_ID | RAND)
- MUK_I = PRF(MUK, ”integrity key constant” | 0xFF | CSB_ID | RAND)
- MUK_S = PRF(MUK, ”salting key constant” | 0xFF | CSB_ID | RAND)

Where | denotes concatenation.

Once the MSK is extracted from the KEMAC payload, it is stored in the UE to be used as a pre-shared key for the MTK delivery messages.

4 MTK delivery and MSK derivation

In this section it is assumed that the MSK is installed in the UE. The MSK is used as a pre-shared key in the MIKEY protocol. When the multicast message containing an MTK reaches the UE, the UE runs MIKEY with the MSK as pre-shared key. This results in that MIKEY internally runs the PRF to derive MSK_C, MSK_I and MSK_S as follows:

- MSK_C = PRF(MSK, ”encryption key constant” | 0xFF | CSB_ID | RAND)
- MSK_I = PRF(MSK, ”integrity key constant” | 0xFF | CSB_ID | RAND)
- MSK_S = PRF(MSK, ”salting key constant” | 0xFF | CSB_ID | RAND)

4.1 Streaming Key derivation

In the streaming case the MTK is extracted from the KEMAC payload, and is in MIKEY terminology a TEK. This means, as stated above, that it is passed directly to SRTP (as a SRTP master key).

The KEYMAC payload also includes a salt, which is sent along with the MTK to SRTP (see [3] for a discussion on the need for salt in MBMS). Instead of sending a separate salt together with the MTK, it could of course be generated from the MTK together with the SRTP master key, but then the MTK would have to be longer (to provide sufficient entropy). If the salt and SRTP master-key where derived from the MTK, they would be cryptographically independent, which should be enough.

4.2 Download Key derivation

No protection scheme has yet been agreed for the download case. However, all current proposals require separate keys for encryption and integrity as input. Hence, we have to make use of

MIKEY's mechanism for deriving several keys from one. The PRF once again comes in to play, as follows:

- MTK_C = PRF(MTK, "encryption key constant" | CS_ID | CSB_ID | RAND)
- MTK_I = PRF(MTK, "integrity key constant" | CS_ID | CSB_ID | RAND)

These keys are then passed to the protection mechanism (possibly together with the salt). Recall that the CSB_ID is defined to carry the Key Group ID in MBMS. CS_ID is set to zero.

6 Conclusion and proposal

The paper has shown how MBMS values can be plugged into MIKEY (and how MIKEY deals with these values internally) to achieve the delivery of the MSK and MTK and how further key-derivations are to be used.

We propose that the key derivation functionality of MIKEY (the default PRF) is used in MBMS, since introducing a new PRF would require that the security of this PRF would have to be examined. If an existing PRF is used, it may have to be modified to fit into MIKEY, and the changes would require a new analysis of the PRF. The PRF of MIKEY has been under review in the IETF for approximately three years already.

A CR [4] implementing the changes to TS 33.246 in accordance with this discussion paper is also submitted to the meeting.

7 References

[1] Arkko et. al., "Multmedia Internet KEYing (MIKEY)", RFC3830, IETF
[2] Dierks and Allen, "The TLS Protocol", RFC2246, IETF
[3] Ericsson, "The need for and use of salt in MBMS streaming", S3-040xxx
[4] Ericsson, "MBMS Key processing", S3-040xxx