3GPP TSG SA WG3 Security — S3#35 **S3-040798**

St Paul's Bay, Malta, October 5-8, 2004

Source: **Siemens**

Title: **Reliable (S)RTP index synchronization for MBMS streaming**

Document for: **Discussion and Decision**

Agenda Item: **MBMS**

1 Introduction and problem statement

This contribution discusses the use of the SRTP-index [ROC (Roll-over counter) and RTP SEQ] within key management messages for MBMS streaming and the necessity to have a synchronization mechanism. Section 3.3.1 on 'Packet Index Determination, and ROC, s_l Update' [RFC 3711] highlights following issues (See Appendix for a complete extract of Section 3.3.1):

- **SRTP implementations use an "implicit" packet index for sequencing, i.e., not all of the index is explicitly carried in the SRTP packet**.
- **At the setup of the session, the ROC MUST be set to zero.**
- **Receivers joining an on-going session MUST be given the current ROC value using out-of-band signaling such as key-management signaling**.
- **After a re-keying occurs (changing to a new master key), the rollover counter always maintains its sequence of values, i.e., it MUST NOT be reset to zero**.

Section 8 of [RFC3711] makes following recommendation:

- **Sending the RTP sequence number in the key management may be useful**

2 SRTP index determination in different scenario's

The MBMS multicast receiver shall be able to reliably determine the SRTP index in different scenario's. Two of them are described below.

1) The MBMS user has performed an MBMS application layer joining after the start of the MBMS session (I.e. the RTP session(s) are already ongoing).

   In addition to the ptp delivery of the MSKs, the MBMS receiver needs to obtain the MTK and the ROC. The RTP SEQ number can be determined from the RTP packet and it assumed the ptm stream contains enough MTK MIKEY messages to enable a fast SRTP session synchronization.

   The MIKEY protocol has a built-in payload (I.e. CS ID map info for SRTP) within the MIKEY common header which allows transferring the SRTP Roll-Over Counters. It is assumed that the CS ID map info is only intended for the MSK key transfer in ptp and not includes to intended for the MTK key transfer in ptm. It could be considered to supply the full RTP index over the ptp

connection[1], but as MIKEY has no such capabilities an http field would need to be defined for this.

2) An MBMS user has been out of UMTS radio coverage some time and has lost ROC-synchronisation. It is assumed that the same RTP session is still ongoing[2].

   There may be different solutions to reliably synchronize the ROC[3]. The user could initiate an http request to get the ROC or the ROC could be multicasted together with key management messages from time to time.

   A first solution could reuse the http based solution which would be needed anyhow for late entrants (scenario 1). A disadvantage is the need for a ptp connection, but the advantage is that the user could be synchronized fast. In order to save standardization effort it is proposed here to rely on MIKEY defined procedures as much as possible. Within the MIKEY message common header the ROC value is included. The actual MSK key payload does not need to be processed at the UE it the UE only needs the ROC.

   The second solution delays the synchronization until a ROC-sync message is multicasted (used protocol has to be defined) and is more efficient in use of radio resources then the first solution. The introduced delay depends on the frequency of the ROC-sync update.

   For a third possible solution it is proposed also to include ROC values within the ptm MIKEY MTK messages. A disadvantage is the increased overhead of the key messages. Possibly as a further enhancement an MBMS CS ID map info for SRTP could be defined for sending only the ROC (strip other policy information away of that payload). The introduced delay of synchronization depends on the frequency/redundancy of the MTK MIKEY messages. The use of this payload may be an operator decision.

3 Conclusions

This contribution discussed the need for a Reliable (S)RTP index synchronization for MBMS streaming. It is proposed to adopt a solution based using the CS ID map info within the multicasted MTK messages. It is proposed to approve the change request which is available in attach to this contribution. Further optimizations of this solution could be done, in which case the attached CR could be used as a basis at the next SA3-meeting.

---

1 See section 8 recommendation

2 Otherwise SSRC would be changed. Note that ROC is reset for each RTP session start

3 Note that RFC3711 provides a basic mechanism to synchronise the RoC on roll-over of the SEQ but there will be cases where this does not work. See also appendix of this contribution

4 Appendix (extract from RFC3711)

4.1 section 3.3.1

SRTP implementations use an "implicit" packet index for sequencing, i.e., not all of the index is explicitly carried in the SRTP packet. For the pre-defined transforms, the index i is used in replay protection (Section 3.3.2), encryption (Section 4.1), message authentication (Section 4.2), and for the key derivation (Section 4.3).

When the session starts, the sender side MUST set the rollover counter, ROC, to zero. Each time the RTP sequence number, SEQ, wraps modulo 2^16, the sender side MUST increment ROC by one, modulo 2^32 (see security aspects below). The sender's packet index is then defined as

i = 2^16 * ROC + SEQ.

Receiver-side implementations use the RTP sequence number to determine the correct index of a packet, which is the location of the packet in the sequence of all SRTP packets. **A robust approach for the proper use of a rollover counter requires its handling and use to be well defined**. In particular, out-of-order RTP packets with sequence numbers close to 2^16 or zero must be properly handled.

The index estimate is based on the receiver's locally maintained ROC and s_l values. **At the setup of the session, the ROC MUST be set to zero. Receivers joining an on-going session MUST be given the current ROC value using out-of-band signaling such as key-management signaling**. Furthermore, the receiver SHALL initialize s_l to the RTP sequence number (SEQ) of the first observed SRTP packet (*unless the initial value is provided by out of band signaling such as key management*).

On consecutive SRTP packets, the receiver SHOULD estimate the index as i = 2^16 * v + SEQ, where v is chosen from the set {ROC-1, ROC, ROC+1} (modulo 2^32) such that i is closest (in modulo 2^48 sense) to the value 2^16 * ROC + s_l (see Appendix A for pseudocode).

After the packet has been processed and authenticated (when enabled for SRTP packets for the session), the receiver MUST use v to conditionally update its s_l and ROC variables as follows. If v=(ROC-1) mod 2^32, then there is no update to s_l or ROC. If v=ROC, then s_l is set to SEQ if and only if SEQ is larger than the current s_l; there is no change to ROC. If v=(ROC+1) mod 2^32, then s_l is set to SEQ and ROC is set to v.

After a re-keying occurs (changing to a new master key), the rollover counter always maintains its sequence of values, i.e., it MUST NOT be reset to zero.

As the rollover counter is 32 bits long and the sequence number is 16 bits long, the maximum number of packets belonging to a given SRTP stream that can be secured with the same key is 2^48 using the pre-defined transforms. After that number of SRTP packets have been sent with a given (master or session) key, the sender MUST NOT send any more packets with that key. (There exists a similar limit for SRTCP, which in practice may be more restrictive, see Section 9.2.) This limitation enforces a security benefit by providing an upper bound on the amount of traffic that can pass before cryptographic keys are changed. Re-keying (see Section 8.1) MUST be triggered, before this amount of traffic, and MAY be triggered earlier, e.g., for increased security and access control to media. Recurring key derivation by means of a non-zero key_derivation_rate (see Section 4.3), also gives stronger security but does not change the above absolute maximum value.

On the receiver side, there is a caveat to updating s_l and ROC: if message authentication is not present, neither the initialization of s_l, nor the ROC update can be made completely robust. The receiver's "implicit index" approach works for the pre-defined transforms as long as the reorder and loss of the packets are not too great and bit-errors do not occur in unfortunate ways. In particular, 2^15 packets would need to be lost,

or a packet would need to be 2^15 packets out of sequence before synchronization is lost. Such drastic loss or reorder is likely to disrupt the RTP application itself.

The algorithm for the index estimate and ROC update is a matter of implementation, and should take into consideration the environment (e.g., packet loss rate) and the cases when synchronization is likely to be lost, e.g., **when the initial sequence number (randomly chosen by RTP) is not known in advance (not sent in the key management protocol) but may be near to wrap modulo 2^16**.

A more elaborate and more robust scheme than the one given above is the handling of RTP's own "rollover counter", see Appendix A.1 of [RFC3550].

4.2 Section 8 Key management considerations

Sending the RTP sequence number in the key management may be useful e.g., when the initial sequence number is close to wrapping (to avoid synchronization problems), and to communicate the current sequence number to a joining endpoint (to properly initialize its replay list).

3GPP TSG-SA WG3 Meeting S3#35
St Paul's Bay, Malta, October 5-8, 2004

Tdoc ⌘Att_S3-040798

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.246** **CR** **011** ⌘ **rev** **-** ⌘ 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⌘ ☐ ME [X] Radio Access Network ☐ Core Network [X]

Title:	⌘	SRTP index synchronisation within ME
Source:	⌘	Siemens
Work item code:	⌘	MBMS
Date:	⌘	28/09/2004
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:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Once the MBMS receiver has lost SRTP index synchronisation on a stream then he will be unable to further decrypt and authenticate the SRTP packets of the same SRTP session.
Summary of change:	⌘	Add the missing functionality: - Specify how to synchronise the SRTP Roll-over-counter
Consequences if not approved:	⌘	It will remain unspecified yet how an MBMS receiver can synchronise the SRTP Roll-over counter, and hence this might lead to the inability of MBMS streaming receivers to reconvene the MBMS session after being out of radio coverage for some time.

Clauses affected:	⌘	6.6.2

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

Other comments:	⌘	

===== BEGIN CHANGE =====

6.6.2 Protection of streaming data

6.6.2.1 Usage of SRTP

When it is required to protect MBMS streaming data SRTP (Secure Real-time Transport Protocol) as defined in [11] shall be used. The MTK is carried to the UEs from the BM-SC using MIKEY [9] with extensions defined according to this specification. MTK shall be used as the master key in SRTP key derivation to derive the SRTP session keys as defined in chapter 4.3 of [9]. The correct MTK to use to decrypt the data is indicated using the MKI (Master Key identifier) field, which is included in the SRTP packets as defined in [11]. The form of MKI shall be a concatenation of Network ID, Key Group ID, MSK ID and MTK ID, i.e. MKI = (Network ID || Key Group ID || MSK ID || MTK ID).

If the SRTP packets are to be integrity protected, the SRTP authentication tag is appended to the packets as defined in [9].

SRTP security policy parameters, such as encryption algorithm, are transported in MIKEY Security Policy payload as defined in chapter 6.10.1 in [9].

6.6.2.2 Packet processing in the UE

When the SRTP module receives a packet, it will check if it has the MTK corresponding to the value in the MKI field in the SRTP cryptographic context.

NOTE: The SRTP module does not need to interpret the MKI field semantics. It only checks whether it has the MTK corresponding to the MKI value.

If the check is successful, the SRTP module processes the packet according to the security policy.

If the SRTP module does not have the MTK, it will request the MTK corresponding to the MKI from the key management module. When the key management module returns a new MTK, the SRTP module will derive new session keys from the MTK and process the packet. However, if the key management module does not have the MSK indicated by MKI, then it should fetch the MSK using the methods discussed in the subclause 6.3.

If the SRTP module has lost synchronisation on the ROC (Roll-over counter) of the SRTP stream, it shall wait for the next MTK update message received within the ptm stream. The BM-SC shall deliver the current ROC-value within the CS ID map info payload of the MIKEY common header payload.

The below flow shows how the protected content is delivered to the UE.

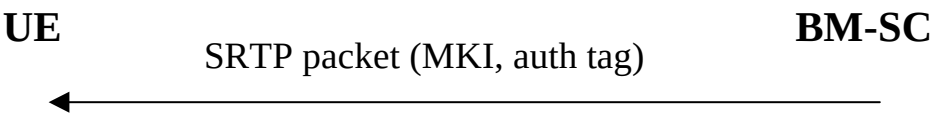

Figure 6.8: Delivery of protected streaming content to the UE