3GPP TSG SA WG3 Ad hoc **S3z030026**

3 – 4 September 2003

Antwerp, Belgium

Agenda Item: MBMS

Source: Ericsson

Title: Introducing SRTP in TS 33.246

Document for: Discussion/Decision

1. Scope

This contribution discusses and describes the use of SRTP as a security protocol for MBMS streaming services. Ericsson provided with a pseudo CR to SA3 in [1] to show that a concrete solution for streaming MBMS data is available. Ericsson makes the suggestion to adopt SRTP for streaming services for MBMS as a working assumption based upon the following arguments:

- A comparison with SRTP and other protocols made by Ericsson at earlier meetings suggests that SRTP is a strong candidate for streaming services
- Harmonization with the IETF work i.e. work being progressed by the MSEC group
- 3GPP TSG SA4 will consider maximizing the re-use of existing features which includes RTP for PSS
- SRTP has passed IESG last call and IESG review and is in practice approved by IETF

2. Introduction

Background from SA3#29

In SA3#29 Ericsson presented contribution [1] and related pseudo CR, which proposed to adopt SRTP and MIKEY for MBMS. Proposal was not agreed due to concerns raised in the meeting e.g. due to that the key management protocol was not inline with the proposal currently discussed in 3GPP2. However since there is a lack of indication of what protocols to use it is difficult to make any detailed judgment of the whole system impacts based on [10]. In [10] it was also not clear what type of redundancy (if any) is required e.g. use of FEC (Forward Error Corrections) or similar techniques to mitigate the issue related with bit errors.

This contribution describes that SRTP can be used as security protocol for streaming MBMS media. Should the Ad Hoc endorse the working hypothesis to include SRTP for protection of streaming services for MBMS Ericsson volunteers to further evolve [1] based on feedback received by the Ad Hoc meeting to the SA3#30 meeting for inclusion in the TS.

Earlier background

In SA3#25 Ericsson presented contributions [3] and [4] which proposed to adopt SRTP and MIKEY for MBMS.

[4] discussed MIKEY and it was compared to two other multicast key management protocols, namely Group Domain of Interpretation (GDOI) [5] and Group Security Association And Key Management Protocol (GSAKMP-light) [5]. MIKEY was found the most efficient and best suitable for MBMS since it is using pre-shared keys with symmetric cryptography. MIKEY was proposed for MBMS.

In [3] SRTP was compared against IP sec and radio –level multicast security. The contribution proposed SRTP as security protocol for streaming applications for MBMS.

However, SA3 #25 concluded that there were too many open issues regarding e.g. the security architecture and further contributions were requested to progress the technical specification. At that time the TS was not mature enough for specific protocols to be included.

In meetings #27 and #28 SA3 agreed on some important security architecture issues, namely that the encryption of MBMS traffic shall be done between UE and BM-SC and that the BM-SC shall be the entity to generate and distribute the traffic encryption key (TEK) to the UEs [6]. Today many issues are still to be specified, e.g. regarding user authentication, charging models (and related keying mechanisms) and Gmb interface functionality.

Ericsson presented a discussion paper [7] on the status of MIKEY [8] and SRTP [9] in IETF in SA3#28. These protocols are strong candidates for key management and security protocols for MBMS and they are likely to get RFC status during 2003.

2. Discussion

Comparison of security methods

In addition to SRTP, so called BAK scheme [10] has been presented for SA3. The present chapter compares these two methods for securing MBMS data. These two security methods prove to be quite similar. The essential difference in the security methods seems to be where in the UE different functions are performed and what is the trust model between the user and the network.

Both SRTP and the BAK scheme have a master key, that needs to be transferred from the network to users by key management mechanisms (e.g. with MIKEY).

For actual data ciphering both methods use session keys that are derived from the master key. The session keys provide more security with less key management signalling effort since several session keys can be derived from one master key and a compromised session key does not compromise other session keys derived from the same master key. The SRTP and BAK methods differ how the session keys are derived from the master key. SRTP derives the session key from a sequence number and the master key while BAK uses a random value and the master key. The security of the methods is essentially equal if the master key is not compromised. Even though SRTP uses sequence numbers in key derivation, it is not possible to predict future keys if the master key is not compromised.

If an SRTP master key leaks, then all future session keys derived from it can be computed in advance. This cannot be done in the BAK scheme, since one has to wait for the RAND to arrive. However, this does not make a big difference in the methods, since one anyway has to be on-line when the actual media is broadcast. Therefore, an attacker can still just publish the master key to other users, who can still decrypt on the fly by grabbing the RAND and deriving the session key. Therefore, in both methods, a leaked master key compromises all session keys derived from that master key. One can in fact also argue that SRTP has an advantage in terms of bandwidth, as the information to derive keys need not be signaled explicitly.

However, a compromised master key reveals all session keys derived from it. Therefore it is important that the master key is not compromised. This is a question of trust model and/or secure storage of the master key. If an authorised user or device cannot be trusted not to reveal the master key, the master key should be stored securely. In BAK scheme the master key is stored in UICC and only the derived session key is revealed to the ME. The SRTP method does not specify where the master key is stored or where the session key derivation is done, but if the ME cannot be trusted, also SRTP master key and session key derivation could be placed in a secure storage, e.g. in UICC or some other tamper-resistant storage in the ME. In this sense, the two methods do not essentially differ from security point of view. However, given the expected value of MBMS data in Release 6, Ericsson believes in a trust model where the ME can be trusted in Release 6 timeframe.

Therefore, the question no more seems to be *which method to use*, but *where master key is stored* and *where the session key is derived*, i.e. a question on trust model. There seems to be at least four alternatives

1. In this alternative the terminal is trusted and the master key is stored in the terminal. This is the Ericsson preferred solution for Release 6 timeframe. Considering the value of MBMS content frequent key updates may not be needed

2. In this alternative the terminal is not trusted. The UICC stores the master key and derives the session keys (which may need to be done quite often).We save in the key management signalling since we don’t have to

update the master key very often because the risk for master key compromise is low. However, this would mean new UICC cards and the burden for UICC could be high.

3. In this alternative the terminal is not trusted. The master key is not stored and the session keys are not derived in the UICC We may need more key management signalling. This is because the ME may not be trusted and we may need to update master key more often. We could manage without new UICC cards.

4. A fourth alternative could be a tamper resistant module in the ME, but not the UICC.

A question is also whether so high value content is transmitted over MBMS, that extra security efforts are needed OR whether high value content should use other protection mechanisms such as DRM.

It can be argued that the value of the content determines the lifetime of the master key and the used trust model. For high value content the key lifetime should be shorter than for low value content. The value of expected MBMS content, for example video clips from a football match [15], don't seem to require frequent master key updates even though the key would leak to some users, since the number of users being technically capable of exploiting a leaked key is assumed to be very low. Considering the expected value of the content in Release 6, also the trust model can be such that the terminal can be trusted not to leak the master key, i.e. the terminal is regarded as a closed environment and extra tamper resistant memory is maybe not required.

Given the expected use cases [16] and value of content of MBMS, Ericsson believes that in the short term, i.e. Release 6, trusting the terminal is enough and the master key can be stored in the terminal. Ericsson also requests SA3 to take a standpoint whether the expected value of content is such that trusting the terminal is enough for release 6 or whether other security measures should be taken.

If the MBMS services take off and high value content will be transported by MBMS, the master key could be moved towards the UICC in the later releases. If MBMS proves to be a success in the future and more secure storage is needed for master key, SRTP provides a migration path since SRTP master key and session key derivation could also be included in UICC or some other tamper resistant device.

Selection of security protocol

The selection of the security protocol for MBMS depends heavily on the chosen application and transport protocols that are specified by SA4.

As it can be seen in LS from SA4 [11] in SA3#29, SA4 has been given the ownership of the definition of data types, codecs, formats and transport/application protocols for the MBMS application. To proceed this work SA4 has produced a Work Item Description (WID) [12].

Re-use of existing functionality is cost-effective. In the clauses of the WID the importance of re-use is highlighted:

"The specification work will take into consideration the need to maximize the reuse of existing features of other 3GPP services."

and also in

"Reuse of PSS and MMS features will be considered."

Both release 5 TS 26.234 [13] and draft release 6 TS 26.234 [14] for PSS codecs and protocols define RTP over UDP/IP as transport protocol for continuous streaming media (speech, audio and video).

SRTP (Secure RTP) [9] is a security protocol and a profile of RTP, which can provide confidentiality, message authentication and replay protection to the RTP/RTCP traffic. SRTP can achieve high throughput and low packet expansion. SRTP proves to be a suitable protection for heterogeneous environments. SRTP protocol has been developed especially for securing streaming applications.

Thus, since re-use of features/protocols is highly desirable and PSS uses RTP, it is cost-effective and logical to choose a profile of RTP, i.e. SRTP, as security protocol for streaming MBMS applications.

The security protocol for download MBMS media is FFS.

There exist a couple of SRTP implementations, e.g. by Ericsson.

Status of SRTP in IETF

SRTP has passed IESG last call and is in practice approved by IETF.

3. Proposal

Based on the reasoning given in the present paper it is proposed to select SRTP as the security protocol for streaming MBMS media. Ericsson volunteers to further evolve [1] based on feedback received by the Ad Hoc meeting to the SA3#30 meeting for inclusion in the TS.

4. Conclusion

This contribution has given the reasoning for choosing SRTP as security protocol for streaming MBMS media. Ericsson requests SA3 to take a standpoint whether trusting the terminal is enough for release 6.

5. References

[1] TD S3-030368, Pseudo CR Introducing MIKEY and SRTP to TS 33.246, Ericsson

[2] 3GPP TS 33.246, v 0.2.0 Security of Multimedia Broadcast Multicast Service

[3] TD S3-020533, Security protocol, Ericsson

[4] TD S3-020534, Key management, Ericsson

[5] http://www.ietf.org/html.charters/msec-charter.html

[6] TD S3-030249, Key generation and distribution in MBMS, Ericsson

[7] TD S3-030250, Status of SRTP and MIKEY in IETF, Ericsson

[8] MIKEY: Multimedia Internet KEYing, draft-ietf-msec-mikey-07.txt, work in progress

[9] The Secure Real-time Transport Protocol, draft-ietf-avt-srtp-09.txt, work in progress

[10] TD S3-030356, MBMS Security Framework, Qualcomm

[11] TD S3-030313, LS: Reply to “Reply to Liaison Statement on MBMS Codec Requirements”, Nokia

[12] TD S4-030414, WID for Multimedia Broadcast/Multicast Service (MBMS) codecs and protocols, Nokia

[13] 3GPP TS 26.234, v 5.5.0 PSS Protocols and Codecs

[14] 3GPP TS 26.234, v 0.2.6 PSS Protocols and Codecs, same as TD S4-030567

[15] 3GPP TS 22.146, v 6.2.0 Multimedia Multicast/Broadcast Service

[16] 3GPP TS 22.246, v 0.2.0 MBMS User Services