3GPP TSG SA WG3 Security — S3#31 **S3-030708**
18 - 21 November 2003
Munich, Germany

Agenda item: 6.20

Source: Samsung Electronics

Title: MBMS Traffic Encryption Key gradually Changing and Updating for streaming service

Document for: Discussion and Decision

1. Introduction

MBMS traffic encryption key(TEK) shall be changed regularly for security as well as charging. Due to power off, out of service etc, one legal UE may miss the key updating. For streaming service, it is proposed that the new traffic encryption key shall be gradually changed from the old one and transmitted to the UEs in turn. This makes it possible that those UEs who miss the new key updating still be able to experience the service with QoS-degraded by using the old key for traffic data decryption. Also, it may be helpful for the operator to find out who may leak out the key by using the new key but limiting the new key updating to only some of the users.

2. Discussion

2.1. Miss of key updating

As indicated in current TS33.246[1], “Like any service, the keys that are used to protect the transmitted data in a Multicast service should be regularly changed to ensure that they are fresh…” This key updating can be used to ensure that users who have joined a multicast service, but then left, shall not gain further access to the multicast service without being charged appropriately. It is assumed that one legal UE who has already been correctly charged for the service should be able to receive the updated keys exactly. However, no matter point-to-point or point-to-multipoint or any other mechanisms are adopted for this key updating, some legal UEs may still miss this key updating due to reasons such as power off, out of service or other unclear reasons. In this case, these UE shall have to use the old keys to decrypt the traffic data at least for some time. Especially for streaming service, this wrongly-decrypted traffic data shall give the user a quite bad feel, since this user has definitely paid for this service already.

However, this problem may be solved by carefully defined MBMS traffic encryption keys gradually changing for streaming service, which shall be discussed in detail in the following section 3.

2.2. Keys leakage

There are existing several discussion papers during previous meetings [2][3], comparing the 3 different re-keying methods: simple point-to-point model [4], BAK method [5] and the combined re-keying method [6]. It was clarified that all the 3 MBMS key distribution methods can fulfil general security requirements (all keys are uniquely identifiable, regular change of keys, re-keying etc.). This document shall not make any further analysis about to what extent each method can fulfil these requirements, because they have already been fully analysed during previous meeting. However, it should be noted that one common question for all these 3 methods is that the network cannot find out which illegal UE leaks out the keys in deed. For the simple point-to-point method, if one illegal UE leaks out the common TEK, other UEs may eavesdrop the content free of charging using this common TEK. As for the BAK scheme and the combined method, if BAK is leaked out, other UEs still be able to obtain the current TEK encrypted with or generated from this BAK and thus eavesdrop the content free of charging. On the other hand, it is quite difficult for the network operator to find out at last which illegal UE leaks out these keys, because these keys (TEK and BAK) are the same for every joined UE.

Actually, this problem may be partly solved by carefully defined MBMS traffic encryption keys gradually updating, which shall be discussed also in the following section 4.

3. MBMS TEK gradually changing

As it was already agreed that the TEK used for MBMS data protection should be identifiable, it is further proposed that the new TEK is derived from the old TEK by randomly changing some composing bits; the remaining bits are the same for both the new TEK and the old TEK. Thus, if one legal UE misses the new TEK updating, it shall have to use the old TEK for content decryption at least for some time before it can obtain the new TEK. Since the old TEK is only different from the new TEK with some composing bits, for streaming service, using the old TEK instead only leads to some content bits wrongly decrypted. In this case, for this specific UE, this content error caused by using expired TEK makes no difference with that caused by aberrant transmission of the original content bits. Thus, using this expired old TEK shall also lead to the degraded QoS received by this UE. For example, if the length of TEK is 128 bits and the new TEK is different from the old TEK with only two bits, using the old TEK instead of the new TEK for data decryption shall lead to 1.56% BER for streaming service. And using this same old TEK instead of the next new TEK shall lead to 3.12% BER, using this same old TEK instead of the third consequent new TEK shall lead to 4.69% BER… Thus, this gradually changed MBMS TEK may help the UEs continue receiving the successive streaming service even they may miss the TEK updating.

Furthermore, it can also be provided beneficial for the operators. If users are roughly “cut off ” from the service because TEK is changed and they didn’t pay for the new TEK, they may become angry and refuse to recharge for the remaining content. In this case, these users are eventually missed. But if the MBMS TEK is gradually changed, these users may rediscover some interest in the remaining content and prefer to recharge for this service.

Also, in order to abstract more users, the service provider may hope to provide some “free” time/content of the service for all users at the beginning of the service. The proposed MBMS TEK gradually updating provides one good means for this purpose.

4. MBMS TEK gradually updating

Instead of distribute the new TEK to all UEs, it is proposed to distribute the new TEK only to some of them each time. Thus, although the network uses one TEK for data encryption at the same time, different UEs shall use different versions of TEK for data decryption. In this case, if one illegal UE leaks out the TEK it uses currently, it shall be easier for the network to know which UE it may be, since the knowledge of this TEK is limited to only some specific UEs.

5. Conclusion

Based on the above analysis, the proposed MBMS gradually changing can solve the "miss of key updating" problem, and may be beneficial for the operator for service extension. And the proposed MBMS gradually updating may help the operator to find out who may leak out the keys. Thus we propose to adopt this TEK gradually changing and updating for MBMS key management and adopt the following text proposal:

-------TS 33.246 v0.6.0 ----------

5.2 Key management and distribution

Like any service, the keys that are used to protect the transmitted data in a Multicast service should be regularly changed to ensure that they are fresh. This is even more necessary in a Multicast service, as the need to changed keys can also be driven by a new user joining the service (to stop them being able to decrypt data sent before they joined the service) or a user leaving the service (to stop them being able to decrypt traffic sent after they left the service).

It was agreed that TEK generation and distribution to the UE are performed by the BM-SC. For streaming service, the new TEK is derived from the old TEK by randomly changing some composing bits; the remaining bits shall be kept same for both the new TEK and the old TEK. Based on network operator's decision, the distribution of the new TEK may be limited to only some of the legal UEs.

Editor's note: It needs to be decided if there is to be a minimum amount of traffic that is to be protected with one key, as this puts a lower limit on the frequency of key changes, e.g. one continuous transmission of data. It could also be possible for several of these minimum amounts to be transmitted with changing the key. It is ffs what this minimum amount should be and whether several of these minimum amounts can be transmitted without changing the key.

Editor's note: If all users need to request a key update simultaneously then there may need to be some method of ensuring that all the users do not request a key update at the same time. This mechanism is ffs.

Editor's note: The keys can be distributed to each user receiving the same MBMS service in point-to-point mode when the number of the users is relatively small. And the users receiving the same Multicast service within the same area can also be further combined into one to several subgroups to make it possible that the keys can be given to all users within one subgroup at a time in point-to-multipoint mode.

6. Reference

[1] TS33.236 v 0.2.0, Security of Multimedia Broadcast/Multicast Service

[2] Tdoc S3-030539, Key management considerations for MBMS, Ericsson

[3] Tdoc S3-030580, MBMS – Overhead of the Re-keying, Nokia

[4] Tdoc S3-030368, Introducing SRTP and MIKEY in TS 33.246, Ericsson

[5] Tdoc S3-030360, Levels of Key Hierarchy for MBMS, Qualcomm

[6] Tdoc S3z030020, MBMS – Combined Re-keying Method, Nokia