3GPP TSG SA3 Ad-hoc Meeting **S3z030014**
3 - 4 September 2003
Antwerp, Belgium

Agenda item: 6.3

Source: Samsung

Title: Comparison between ptp re-keying and re-keying based on LKH

Document for: Discussion and Decision

1. Introduction

In principle, MBMS traffic encryption key(TEK) re-keying from the network (mainly BMSC) to UEs can be done in ptp mode or in ptm mode such as LKH. This paper makes some comparison between these 2 modes regarding to re-keying confidentiality, efficiency and complexity, and proposes that ptm re-keying shall be adopted, especially when ptm bearer is used for MBMS data transmission.

2. Discussion

During previous SA3#28 meeting, SA3 has agreed that the MBMS TEK generation and distribution to UE shall be performed by the BM-SC. In principle, this MBMS TEK distribution from the network (mainly BMSC) to UEs can be done in ptp mode or in ptm mode such as LKH. For the ptp TEK distribution, the distribution procedure can be uniform. Whenever BMSC generates one TEK, the network shall need to establish one end-to-end bearer from the BMSC to each UE for TEK transmission.

The ptm TEK distribution requires previous securely some kind of keys shared by a group of users. Thus, the TEK distribution procedure can be divided into 2 phases: the initial TEK distribution and the latter TEK re-keying. During the initial TEK distribution phase, the BMSC shall also need to establish one end-to-end bearer from the BMSC to each UE to transmit these shared keys, which is in the same way as ptp key distribution. Usually, this initial TEK distribution can occur when one UE joins the service.

During the latter TEK re-keying, if there is no UE leaving/joining (UE joining scenario is FFS.) within one group of UEs, the updated TEK can be distributed to this group of UEs in ptm mode, by using the keys which were shared by this group of users only and distributed to these UEs in ptp mode during previous initial TEK distribution phase. If there is UE leaving/joining within one group of UEs before the following TEK re-keying, the updated TEK shall be distributed to each UE within this group in ptp mode, which is in the same way as the initial TEK distribution.

This paper mainly makes comparison between the ptm re-keying case and the ptp based re-keying.

3. Comparison

3.1. Re-keying Confidentiality

In principles, the threats associated with attacks to the re-keying confidentiality includes attack to the UE and eavesdropping over the re-keying path, which are described in the following sub-chapters.

3.1.1 Attack to the UE

As we know, a valid USIM shall be required to access any 3G service including the MBMS service, and the decoding keys used for MBMS data decryption may be generated and/or stored in this (U)SIM card and then passed from this (U)SIM card to the decoder. Thus, one hacker may try to crack the (U)SIM card where these keys shall be generated or stored, or he may try to eavesdrop these keys when they are transmitted from the (U)SIM card to the decoder.

For ptp based re-keying, this hacker may need to crack only one key which is used for TEK deciphering. Once this hacker can obtain this deciphering key, he shall be able to obtain later updated TEKs which are encrypted using this ciphering key. While for LKH based re-keying, this hacker may have to crack all intermediate keys which may be used by this UE for TEK deciphering, because each of these keys can possibly be used depending on actual grouping selection by the network. Thus, this hacker shall have to crack multiple keys compared to just one key when LKH based re-keying is adopted instead of ptp based re-keying. But it should be noted that it may be the similar difficult level to crack the keys stored or generated inside the (U)SIM card no matter whether ptp based re-keying or LKH based re-keying is adopted.

Because no matter ptp based re-keying or LKH based re-keying is adopted, it is likely that only the finial decoding keys shall be transmitted from the (U)SIM card to the decoder, the use of the keys which are associated with re-keying itself shall be limited within (U)SIM card. This means that it is indeed the same difficult level to eavesdrop these keys when they are transmitted from the (U)SIM card to the decoder.

Once one hacker can crack the (U)SIM card or obtain the keys by eavesdropping the keys transmitted from the (U)SIM card to the decoder successfully, the keys used in both ptp based re-keying and LKH based re-keying can be leaked out.

3.1.2 Eavesdropping over the re-keying path

Eavesdropping over the re-keying path may include eavesdropping over the air and eavesdropping within the core network. This kind of intruder may have successfully obtained the deciphering keys which shall be used for TEK re-keying deciphering. Thus, if this intruder can obtain the ciphered TEK re-keying message successfully, he shall be able to obtain the updated TEKs using these deciphering keys. When ptp based re-keying is adopted, the intruder shall need to try to monitor messages destined to the original legal UE all the time, because the ptp re-keying message can happen at anytime and this kind of intruder may have no any knowledge of this. This is difficult for the intruder and brings extra cost to the intruder even it is feasible. As for the ptm re-keying, the intruder may have some knowledge of when the re-keying message shall be given out, because the schedule information for the ptm

re-keying messages should be open to all (privileged) users in one group. This may be easier for the intruder to obtain the ciphered TEK re-keying message.

On the other hand, the intruder may have no knowledge of these deciphering keys and have to crack the ciphered TEK re-keying message. This scenario is something similar to cracking the (U)SIM card. After obtaining the ciphered TEK re-keying message, for ptp re-keying, this intruder shall need to crack only one key; while for ptm re-keying, this intruder may have to crack all intermediate keys which may be used to cipher the re-keying message by the network. It is obvious that the latter shall be more difficult for the intruder.

It should be noted that frequent re-keying is helpful for re-keying confidentiality.

3.2 Efficiency

If ptp based re-keying is adopted to carry out one MBMS TEK updating procedure to N users, it is quite obvious that N messages shall be needed to transmit the updated TEK to each of these N users. While for ptm based re-keying, in general, with a binary tree for N users, the number of messages required to update the key tree structure, if a user leaves, is 2ld(N)-1, i.e. with $N=2^{32}$ =about $4x10^9$, the number of messages is only 63, i.e. a highly significant reduction of the number of messages is achieved compared with e.g. p2p messages. The number of keys, which each user has to store, is ld(N)+1, i.e. for $N=2^{32}$, 33 keys would have to be stored. For k-ary trees the number of messages is k*log_k(N)-1 , and the number of keys to store is log_k(N)+1, where log_k is the logarithm refering to base k, ld=log_2, logarithm dualis. Thus, it is obvious that LKH based re-keying is more efficient than ptp based re-keying, especially when the number of users is large.

3.3 Complexity

It is also quite obvious that for ptp based re-keying, one UE shall need to keep only one deciphering key at the same time. UE shall used this key for deciphering whenever one ciphered MBMS TEK re-keying message is received. But for LKH based re-keying, one UE shall have to keep multiple intermediate keys and know which key is for which group. In this means, LKH based re-keying mode is more complex than the ptp based re-keying mode.

Actually, the complexity of LKH scheme is quite related to the key hierarchies. The complexity shall also be reduced as the key hierarchies are reduced, while at the same time, the efficiency is reduced as well. In the end, its complexity and efficiency are the same as ptp based re-keying when the key hierarchies is reduced to 2 (i.e. no any intermediate keys at all) in the end. Thus, the costs of complexity and efficiency should be balanced as the number of users increases.

3.3.1 Multiple service coexistence

As we know, many different MBMS services may exist at the same time within one UE's home network. And depending on UE's capability, user may select to join multiple services and receive them at the same time. For example, one user may wish to read some real-time news provided by one content provider while listening to one living concert provider by another content provider. It is quite obvious that different TEKs shall be used for these different services. Thus, this UE should store all these keys and know which key is for which service. This scenario is quite similar to the keys storage scenario in

LKH based re-keying. Samsung has another contribution[1] talking about this issue. As UE may own the capability to support multiple services coexistence case, it can also be updated to support LKH based re-keying with very minimal modification.

4 Conclusion

As a result of the above analysis, we can conclude that as to re-keying confidentiality, LKH based re-keying is at least in the same security level with the ptp based re-keying, and LKH based re-keying is more efficient than the ptp based re-keying. LKH based re-keying is also more complex than the ptp based re-keying, but some UEs may be updated to support LKH based re-keying with very minimal updating. Thus, we propose the following recommendations:

1) SA3 should develop the MBMS key management and distribution mechanisms based on this LKH principles;

2) It's up to the operator to decide whether ptp based re-keying or LKH based re-keying shall be adopted for one specific MBMS service, maybe depending on the number of users for this service.

5 Reference

[1] S3-03xxxx, "User grouping for MBMS key distribution" from Samsung in SA3 Ad hoc