3GPP TSG SA WG3 Security — S3#29 **S3-030349**
15 - 18 July 2003
San Francisco, USA

Agenda item: 7.20 MBMS

Title: MBMS re-keying: PTP with periodic re-keying

Source: Huawei Technologies

Document for: Discussion and Decision

1 Introduction

This contribution focuses on MBMS re-keying. The process of re-keying can be either simple or complex based on the degree of security required by MBMS users, service providers, and content providers. We propose some simple yet effective re-keying schemes for initial MBMS services.

2 Discussion

Point-to-point re-keying provides a simple approach to MBMS re-keying. The level of security provided by point-to-point re-keying should satisfy most users and operators.

However, if all users request the new group key simultaneously, the system could become overburdened. To alleviate this problem, we propose two approaches.

2.1 Approach 1: user's interval and server's interval

The server (root) assigns each user a time interval after which the user can make a re-key request. At the end of each time interval, each user initiates a re-key request and receives the new key. Then at some time later, the server informs all users switch to the new key. Each user repeats his request according to the time interval given to him, and the server repeats the switching command at some larger interval.

The rules for user re-key requests should satisfy several requirements. (1) All re-key requests should not occur at the same time. (2) All users must complete their request based on the time interval assigned by the server, i.e. each user has a specific time to request a new key. (3) The server must respond to initial requests and assign time intervals, possibly the same (which start once the UE receives its time interval), such that the times of subsequent re-key requests will be varied. (4) The users' time intervals are shorter than server's time interval, so that each user can complete a re-key request before the server's switch command.

2.2 Approach 2: user's subgroup and server's interval

The Logical Key Hierarchy (LKH) principle partitions all users into several subgroups and a user's key hierarchy is like a tree in the subgroup. We also can use the concept of subgroups but it is complex to use the key hierarchy to complete the re-keying process.

The server repeats the switch command at the end of server's time interval as described above in section 2.1. Before the switch command, all users should complete requesting the new key. The server can partition it's time interval into several subintervals and partition all users into selected subgroups. At the beginning of each subinterval, the server broadcasts the ID of the subgroup, and then the users in that subgroup request the new key. Once all of the subintervals are processed, each user should have received a new key, and the server's time interval will be at its end. Then the server broadcasts the switch command, and all users switch to the new key.

2.3 Analyses

In the case that a user joins/leaves the service, re-keying does not occur. Re-keying only occurs as described above. Users can join/leave the service only when re-keying occurs. The fact that joining/leaving can't be implemented immediately often occurs in other services too and typically is acceptable to users.

The server's time interval should be determined based on several system aspects such as number of users, level of security, type of MBMS service, etc. The balance of those elements can satisfy the needs of the system in different situations.

For the MBMS key hierarchy, we suggest using an approach outlined in another contribution. The three-level MBMS key hierarchy as proposed by Nokia (S3-030238) is simple and effective. This key hierarchy combined with PTP periodic re-keying provides a complete solution.

Several other more complex techniques for re-keying also have been proposed. For example, Logical Key Hierarchy (LKH) appears to provide a more effective key management scheme when users join or leave the MBMS group. However, the approach is much more complex and when a large number of users leave an MBMS session or need to change keys, the system may become overburdened. Nonetheless, we believe that approaches such as LKH should be explored in more detail and considered for subsequent releases.

3 Conclusion

For initial MBMS deployments, we propose keeping MBMS re-keying simple and easy to implement. We propose adopting the point-to-point re-keying with periodic re-keying as described above. Furthermore, we suggest studying more complex techniques, such as LKH, for subsequent releases.