3GPP TSG SA3 Ad-hoc Meeting **S3z030013**
3 - 4 September 2003
Antwerp, Belgium

Agenda item:	6.2
Source:	Samsung
Title:	Unauthorized access to multicast data analysis
Document for:	Discussion

1. Introduction

Among all the threats associated with attacks on the radio interface, unauthorized access to multicast data is close related to charging. It may greatly affect the operator's income but may be very difficult to be detected at the same time. This proposal makes some analysis about this unauthorized access to the multicast data over the radio interface and concludes that frequent key updating shall be beneficial to keep away this kind of attack.

2. Discussion

As illustrated in current TS33.246, among all threats associated with the attack on the radio interface, unauthorized access to multicast data is one major threat. Some intruders may eavesdrop MBMS multicast data on the air-interface. And some users that have not joined and activated a MBMS multicast service may receive that service without being charged. While some users that have joined and then left a MBMS multicast service may continue to receive the MBMS multicast service without being charged. Basically, these malicious users can be divided into 2 categories: some of them can pass the network authentication and authorization successfully; others cannot pass the network authentication and authorization. The operations of these 2 kinds of malicious UEs are described in the following sections:

2.1 network authentication and authorization passed successfully

No matter what means they may use, the first kind of malicious users can pass or escape the network authentication and authorization and obtain the MBMS TEK for the service successfully without being detected by the network. For example, one malicious user may act as a legal user by (U)SIM clone.

These users can further be divided into 2 kinds: the first kind these of users just listen to the multicast data silently without leaking out the keys after they successfully obtain them. Another kind of these users may give out these keys openly on purpose. e.g. publish them over the internet. It is quite obvious that the latter are more harmful, but the network authentication and authorization procedure cannot detect both these 2 kinds of users or separate them.

2.2 network authentication and authorization not passed

The second kind of users cannot pass or escape the network authentication and authorization successfully. That is, this kind of users cannot directly obtain the MBMS TEKs from the network(mainly BMSC). Thus, these users have to know the correct the TEKs at first before they can decode the encrypted multicast data correctly.

As described above in section 2.1, because the TEKs can be leaked out openly by some intruders who can pass the network authentication and authorization successfully, some users may be able to get these keys from these intruders. But it should be noted that there may exist some delay from the time when these TEKs are leaked out to the time when these malicious UEs obtain these keys. If the TEKs can be updated frequently enough to make them expired before they're obtain by these malicious users, this kind of unauthorized access can be eliminated.

Some users that have joined and then left a MBMS multicast service quickly. Thus these users can continue to receive the MBMS multicast service without being charged, if the MBMS TEKs for this service are not changed after their leaving. But if these MBMS TEKs are updated quickly after these users leaves, this kind of unauthorized access can also be eliminated. These users cannot obtain the updated TEKs further, as they cannot pass the following network authentication and authorization, which the updated TEK distribution procedure shall be based on.

It is imaginable that some malicious users may just try various means to crack the encrypted content themselves. But it is also quite obvious that this kind of unauthorized access is quite difficult for implementation, if power algorithm is adopted for MBMS and the TEKs are updated frequently.

3. Conclusion

As a result of the above analysis, we can see that frequently key updating is helpful to keep away this kind of unauthorized access to the multicast data over the radio interface. This should be taken into consideration by SA3 when evaluating various MBMS user authentication/authorization and MBMS key management/distribution approaches.