3GPP TSG SA WG3 Security — S3#25 **S3-020504**

8 - 11 October 2002

Munich, Germany

Source: **Siemens**

Title: **MBMS Fraud and countermeasures**

Document for: **Discussion**

Agenda Item: **7.19**

Abstract

This contribution analyses the fraud issues that are an inherent property of sharing an MBMS key among MBMS users. Some measures are proposed that could be used to combat that type of fraud and should be taken into account when selecting the appropriate MBMS architecture.

1) The MBMS key and fraud

The MBMS key is an encryption key that is shared by a multicast source in the network[1] and the UEs that joined the multicast group. Its function is to prevent unauthorised UEs from consuming multicast data. The network has the responsibility for MBMS key generation and distribution towards the authorised MBMS consumers.

Fraud issues come into play as the MBMS key is shared between many MBMS consumers and the network, and the network controlled MBMS key lifetime may only be roughly dependent on the dynamic behaviour of UEs that join or leave the MBMS service.

It is assumed that eavesdropping on the communication path, used for transferring the MBMS-key from the key-generation point in the network to the end-user, is much easier than manipulating the terminal. Confidentiality protection of the MBMS-key during transfer to the UE is therefore a primary requirement. The next vulnerable point therefore becomes the UE. A normal user is not able to receive any further MBMS data when he leaves the MBMS group as the UE performs some deactivation procedures. It is the UE that has the key normally, not the user. A malicious user must therefore be able to re-activate the reception procedures on its UE without any signalling with the network. Otherwise he has no use of the remaining lifetime of the MBMS key.

In worst case there will be even malicious users which never had any charging relations with the visited operator/MBMS and which derive (or obtain from malicious colleagues) somehow the MBMS key and therefore may be able to receive the MBMS data without being charged for it. From the above, some fraud scenario's can be defined for which possible countermeasures are proposed in the next clause.

Scenario-1 [SC-1]: A malicious (MBMS subscribed) user still consumes MBMS data after leaving the MBMS service.

Scenario-2 [SC-2]: A malicious (MBMS subscribed) user retrieves the MBMS key and publishes or distributes it to non-subscribed MBMS users that manage to listen in to the MBMS service.

---

[1] The appropriate Node performing that function is still to be selected

Fraud: Free consumption of MBMS data by malicious user.

2) Countermeasures against fraud

This clause analysis the countermeasures to the fraud scenarios listed in previous clause. These techniques cannot eliminate fraud, as it is an inherent property of the applied MBMS encryption, but it can decrease the fraud exposure:

Technique-1: Frequent rekeying.

This addresses mainly [SC-1], and impacts the amount of MBMS distribution messages needed. It indirectly also addresses [SC-2] as publishing/distribution overhead increases on more frequent rekeying.

From a fraud point of view, a rekeying mechanism as often as possible should be chosen, and therefore an approach with a good signalling performance for MBMS key distribution should be selected.

Technique-2: Limiting the key-applicability to smaller areas.

This addresses mainly [SC-2] as it limits the usability of the received MBMS key within the defined areas.

An MBMS-key may have following characteristics:

1) *Shared or non-shared among MBMS-services*: One MBMS key could be used per one or multiple MBMS services. The same key for multiple services reduces signalling load for UEs with multiple joined MBMS services, but on the other hand also gives malicious users the ability to listen in to other MBMS services than the one where the key was obtained.

2) *MBMS-service area wide usage or smaller areas* (Ex. SGSN covered area, RNC-covered area): For MBMS-service area wide usage, the MBMS key is used by all joined UEs for that MBMS-service. The MBMS key therefore applies to all areas of the PLMN where the MBMS service is active. This allows easy fraud by distributing and publishing the MBMS key in public (until re-keyed). From a fraud point of view it is better to have MBMS keys with only 'local' significance. (Ex. SGSN covered area or RNC-covered area). Applicability to smaller areas can lower the benefit of fraud significantly. Note that this makes no statement on the allocation of the MBMS key generation function to a specific network element, but can be argued that keys of 'local' significance could be generated locally (in RNC or SGSN). This not only avoids the security risks in transporting the MBMS-key but also reduces the number of signalling means and helps in distributing the load to multiple entities.

Technique 3: Make it difficult for a malicious user to retrieve the MBMS key from his own terminal.

This addresses [SC-2]. This is an implementation–related technique. It seems independent of the architecture.

3) Conclusion

This contribution did analyse fraud issues related to a 'shared' MBMS key. Three techniques were proposed that limit the fraud exposure for the operator: '*Frequent rekeying*', '*Limiting the key-applicability to smaller areas*' and '*making it difficult to retrieve the MBMS-key from the terminal*'. The findings from a security point of view are that an approach with a good signalling performance for MBMS key distribution should be selected and architectures with local MBMS-key applicability should be preferred.

It is proposed that SA3 communicates these findings to SA2 as important criteria for selecting the appropriate architecture.