3GPP TSG SA WG3 Security — MBMS ad-hoc **S3z030023**
3-4 September 2003
Antwerp, Belgium

Agenda item: MBMS Security

Source: **QUALCOMM Europe**

Title: Integrating Key Management with the Underlying Protocol

Document for: Discussion

1 Introduction

A two-tiered approach for MBMS key management based on that adopted by 3GPP2 has been long proposed in SA3, [1], in order to achieve efficient key management for MBMS [2], [4]. At SA3#29 in San Francisco the question was asked how to integrate this approach with an underlying protocol. This paper aims to initiate discussion about which approaches which may be taken.

2 Discussion

We begin with a taxonomy of approaches which may be taken to carrying out this integration:

1. Payload Encapsulation.
A new IP-level protocol number and header is defined for broadcast keyed traffic. The header contains:
* broadcast key material
* the protocol number of the payload

This header is inserted between the IP{4,6} header and the payload. This mechanism is widely used (e.g. IPSEC transport mode) and will work with any transport protocol.

2. Protocol Extension.
A method for including the keying material in each target transport protocol is defined. There are two sub cases:

a) Invariant: the protocol is unchanged because it was designed to carry such material, or to be transparently extended, and

b) Variant: a new variant of the protocol must be defined to carry the material.

The invariant approach guarantees interoperability, while protocol variants may or may not be interoperable. Thus the former is preferred.

3. Header Extension.

A new IPV6 extension header (or IPV4 option) may be defined to carry keying material. While this would work, it is an inappropriate confusion of transport and network layers. This approach is not recommended.

4. Out of Band Negotiation.

An additional keying protocol may be defined to operate concurrently with the transport. The transport protocol is, therefore, unaffected. This is attractive from the perspective of low impact on existing software, however the price is the need for each network peer to implement an entirely new negotiation protocol. The total cost of this approach is therefore substantially higher than the abovementioned alternatives.

5. Hacks.

There are all sorts of places that one could hide the keying data (ie.trailers, padding fields, etc). These are all fundamentally unattractive as they will erode interoperability of differing implementations.

3 An Example: SRTP

As an example, one approach to be taken may be to use SRTP [6] with an invariant protocol extension. The current internet draft appears particularly amenable to supporting the proposed MBMS key hierarchy: the format of an SRTP packet includes an optional Master Key Indicator field MKI which we could take for the key indicator (SK_RAND,BAK_ID) proposed in [3]. The use of this MKI would then be as described in [3], Section 6.2.

One consideration to improve the quality of service may be to forewarn the ME of a change in SK by sending in advance packets with the upcoming MKI, but essentially no payload, so that the UICC may compute SK prior to the arrival of any content encrypted with that SK.

4 Conclusion

A number of approaches may be taken to integrate the proposed MBMS key hierarchy with the underlying secure transport protocol, and further work may be detailed depending on which protocols are targets for support.

5 References

[1] Draft 3GPP2 Broadcast/Multicast Security Proposal, Qualcomm, S3-020501.

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

[3] CR to 33.246, submission to SA3 MBMS ad-hoc, Antwerp.

[4] Updating Encryption Keys for MBMS, submission to SA3 MBMS ad-hoc, Antwerp.

[5] USIM Enhancements for MBMS Support, SchlumbergerSema, T3-030599.

[6] Baugher et al, Secure Real-Time Transport Protocol, IETF draft.