3GPP TSG SA WG3 Security — S3#33 **S3-040230**
10 - 14 May 2004
Beijing, China

Source: **Ericsson**

Title: **On the need for integrity and source origin authentication in MBMS**

Document for: **Discussion/Decision**

Agenda Item: **MBMS**

1. Scope

This paper discusses the need/sufficiency of integrity protection and source origin authentication in MBMS.

2. Introduction

At SA3 #32, the need for integrity protection in MBMS was discussed and questioned. The argument was that since MBMS uses a group key, integrity does not add much protection, as any group member can forge messages from the BMSC. While one cannot disagree with the analysis, we think the conclusion is premature, and possibly even incorrect. Rather than showing that integrity is not useful, the arguments above shows that *integrity may not be sufficient*. Below, we give some arguments for why integrity should not immediately be discarded, and why even source origin authentication (SOA) may, in fact, be required.

3. Discussions

3.1 Threats from lacking SOA

3.1.1 General Threats

As decided at SA3 #31 (see the final meeting report) a multi-level key management approach is suggested, where lower level media protection keys are distributed using a higher level group key.

Now, without integrity/SOA, as noted, any member of the group can forge messages from the BMSC. This includes, not only media, but also third-level key updates. This implies that group members can create DoS attacks to other members (by sending fake re-key messages) and therefore, in a sense, can also "hijack" or take over the session at that point in time. Given that the current trust-model is that end-users are not trusted not to disclose keys to non-members, it is not clear whether they can be trusted not launch attacks as those above. Admittedly, the attacks mentioned here *may* be technically somewhat more difficult, but we would not disregard the risks too carelessly.

If there is no integrity/SOA, it is also possible for an attacker to send bogus packets, with randomly chosen key identifiers. This would effectively cause a DoS attack against the BMSC, since all terminals receiving these packets would issue a request for the new key.

3.1.2 Application-specific Threats

MBMS is likely to be used not only for "entertainment" type services with relatively low value content. Some possible, near future applications include distribution of stock market quotes, public emergency messages, etc. In both of these cases, it is clear that lack of SOA can be potentially catastrophic since it may trick the user into making seriously

incorrect decisions. We propose that threats in possible future applications of MBMS must be better understood before discarding the need for SOA.

4. Short Technical Background on SOA

Generally, SOA cannot be achieved with symmetric keys, public key technology is needed, since one must make sure that only one party has the key that authenticates the messages. This seems to make SOA infeasible for MBMS. However, there are some promising "hybrid techniques". Specifically, TESLA [2] is one such technique. Here, a hash chain is used, $h_j = h(h_{j-1})$, j = 0,1, …, n by the sender together with a (single) digital signature on h_n. This signature and h_n are distributed to the group at session start. Somewhat simplified, h_{n-1} is used as a key to authenticate (by a symmetric MAC) the first message sent. The next message is authenticated using h_{n-2} and in addition, this message "reveals" h_{n-1}. This means that the group can now (slightly delayed) authenticate the first message by checking the MAC, computing the hash chain forwards and check that (the previously signed) h_n is obtained. On the third message, the second message can be authenticated etc. The actual solution is somewhat more complicated, but the general idea is the same.

For the specific use of TESLA together with SRTP [1], an IETF Internet draft is in progress, [3]. The combination of TESLA with SRTP is particularly advantageous since it allows:

- The immediate verification that the message is from *somebody* within the group (by SRTP's normal integrity mechanism).
- The slightly delayed *true* source origin authentication.

This limits DoS attack effects by outsiders.

5. Short Status Report on Standardization

The work on the TESLA protocol progresses rather slowly in IETF, and it is not known when it will reach RFC status. The SRTP support for TESLA [3] was submitted as a 00-draft February 2004.

6. Conclusion and Proposal

We believe that omitting integrity protection and SOA would be a premature decision, and some analysis should be made to assess the threats involved. We do not see insurmountable technical problems *if* SOA is found to be required.

7. References

[1] Baugher et al: "The secure Real-time transport protocol", RFC 3711, IETF.

[2] Perrig, Canetti, Song, Tygar, and Briscoe, "TESLA: Multicast Source Authentication Transform Introduction", draft-ietf-msec-tesla-intro-01.txt, work in progress.

[3] Baugher and Carrara: "The Use of TESLA in SRTP", draft-ietf-msec-srtp-tesla-00.txt, work in progress.