3GPP TSG SA WG3 Security S3-010354
Meeting #19
London, 4 – 6 July, 2001

Source: Siemens AG

Title: MAP security threats and policy requirements

Document for: Discussion / Decision

Agenda item: 7.1, MAP security

Abstract

This contribution shows that, unless certain security policy requirements are fulfilled, PLMNs implementing MAP security may remain vulnerable against active attacks even if all other operators support MAP security as well. These security policy requirements are derived from the corresponding threats. Furthermore, this contribution proposes text to accommodate a request by SA#10 (Dec00) to include a warning about MAP security that the mechanism is only useful if all interconnected operators also implement MAP Security.

1 Introduction

In TD S3-000688 "Introduction of MAP security", presented and approved at S3#16, there was a discussion why MAP security could be rendered largely useless if no cut-off date for the introduction of MAP security was introduced after which all operators had to at least support protection mode 1 (see section 2).

This contribution shows that, unless certain security policy requirements are fulfilled, MAPSec could remain largely useless against active attacks even if all operators supported MAP security. These security policy requirements are derived from threats which may be realised if the requirements are not fulfilled (see section 3).

What the earlier discussion about a cut-off date for the introduction of MAP security and the new proposals in this contribution have in common is that they require security to be implemented uniformly across all operators in a specific sense. In particular, a cut-off date is required when using the fallback indicator.

2 Introduction of MAP security and the definition of a cut-off date

We briefly recapitulate the earlier discussion at S3#16.

We quote from the conclusions of TD S3-000688: "It follows from the discussion in this contribution that the agreement on a cut-off date for the introduction of MAP security with protection mode 1 in all UMTS (and preferably also GSM) PLMNs is necessary. If no such agreement is reached, the degree of protection even in PLMNs supporting MAP security is likely to be quite limited."

The discussion in TD S3-000688 showed that attackers could modify the source/destination address of a MAP *send authentication info* message from that of a MAPSec protected PLMN to that of an

unprotected PLMN to obtain authentication vectors of any user, independent of the protection status of the home PLMN and the actual location of the user.

We also quote from the report of SA#10:

"TD SP-000622 LS from SA WG3: Security risks in introduction phase of MAP security. SA WG3 informed TSG SA that work was ongoing to secure MAP for Rel4 and Rel5. The benefit of MAP Security is dependent upon both operators involved in a signalling communication having an acceptable level of MAP Security. To address this problem SA WG3 requested that TSG SA endorse that there is a need for a cut-off date for the introduction of enhanced MAP Security, and to ask the GSM Association to propose a suitable date for the introduction of this. . . . The TSG SA Chairman proposed that some text should be added to the MAP Security specification to advise that the mechanism is only useful if all interconnected operators also implement MAP Security. The competence for the appropriate level of security was a matter for SA WG3. . . . It was proposed that other groups are also considered for the liaison from TSG SA. It was concluded that SA WG3 were requested to ensure that the warning about MAP security is included in the relevant specifications."

The latter request by SA#10 has not been implemented yet in S3 (or other) specifications. Suitable **text is proposed here** for section 4 of TS 33.200 (Principles of MAP application layer security):

"The security measures specified in this TS are only fully useful if all interconnected operators use them. In order to prevent active attacks all interconnected operators must at least use MAPsec with the suitable protection levels as indicated in this specification and treat the reception of all MAP messages (protected and unprotected) in a uniform way in the receiving direction. Additionally this requires the introduction of a cut-off date for this feature, which is to be agreed among operators."

3 MAP security policy requirements

3.1 Cut-off date for fallback to unprotected mode

It was proposed that fallback to unprotected mode should be allowed in the introductory phase of MAP security. The idea is that MAP security functions may cause problems when switched on, so MAP operations could continue unprotected while errors were being eliminated. In this subsection, we do not want to discuss the assumptions underlying this approach or the usefulness of the possibility of such a fallback. Rather, we would like to point to the inherent risk in this procedure.

If an active attacker knows that, for MAP messages sent from a PLMN#1 to a PLMN#2, fallback to unprotected mode is allowed the attacker can simply send an unprotected message to PLMN#2 which will be accepted and, if a response is required, will be answered in an unprotected message. Therefore, an active attacker can mount her attack just as if PLMN#1 was not using MAPSec at all, and, consequently, there is no protection against active attacks for PLMN#1 and PLMN#2 although both may have a working implementation of MAPsec. Note also that, for unprotected messages without security header, the receiving MAP network entity generally does not know the source PLMN-Id (cf. section 3.3). The situation strongly resembles that for the introduction of MAP security when only some operators have already deployed MAPsec. Not surprisingly, the proposed countermeasure is also the same. This leads to the following requirement:

Req 1: A particular PLMN shall disallow fallback to unprotected mode for its MAP communication with all other PLMNs after a certain cut-off date.

3.2 Uniformity of protection profiles

If one PLMN does not use the same protection profile with all other PLMNs, there may be security problems. Let us look at the following example:

If PLMN #1 agrees on protection profile C with PLMN#2 and on protection profile E with PLMN#3 for the invoke components sent towards PLMN#1 then the following can happen: protection profile C provides protection for protection group 3 (Authentication information in handover situations), but not for protection group 4 (Non-location dependant HLR data), whereas for protection profile E the converse is true. Now, if an active attacker wants to change non-location dependant HLR data in

PLMN#1 she invokes the operation “AnyTimeModification“ spoofing the source PLMN-Id to become that of PLMN#2. The message will be accepted because invocations of “AnyTimeModification“ from the source PLMN#2 do not require protection according to the protection profile. The fact that the operation “AnyTimeModification“ invoked by PLMN#3 is protected does not prevent any active attack.

In a similar fashion, an attacker could exploit the difference in the protection profiles if he wanted to gain access to Authentication information in handover situations.

The same problems (only worse) occur, of course, if protection profile A (no protection) is mixed with some of the other profiles.

This leads to the following requirement:

Req 2: In order to ensure full protection, a particular PLMN shall use the same protection profile for its MAP communications with all other PLMNs. In particular, full protection is not ensured when protection profile A (no protection) is used with some source/destination PLMNs and other profiles are used with other source/destination PLMNs.

Note 1: according to what was said in section 2, the use of protection profile A (no protection) should be disallowed after a certain cut-off date anyhow.

Note 2: the following objections might be raised against the above considerations: if there was a set of PLMNs secured by means other than MAPSec, e.g. by IPSec for IP-based MAP, then why should the use of protection profile A (unprotected) not be allowed for communication among these PLMNs under the condition that MAPSec protection was still required for communication with other PLMNs? The answer is that this would be only admissible if it could be assumed that there was a cross-checking of the consistency of addresses across the protocol layers, i.e. that it was guaranteed that the PLMN-Id in the MAP security header topologically corresponded to the IP address of the IP packet in which the MAP message was sent. It has been the general assumption on MAP security, however, that the protocol layers are independent and that there is no reliable binding between the addresses visible at the MAP layer and the topologically significant addresses at lower layers. Then active attacks could still be mounted as follows: the attacker sends a MAP message (e.g. invocation of *send authentication info*) from outside the IPSec protected domain to a network entity inside the IPSec protected domain, but with a source PLMN-Id in the MAP security header corresponding to a PLMN also inside the IPSec protected domain. If the MAP protection profile did not require MAPSec protection for this source PLMN-Id then the response would be sent unprotected by MAPSec, but to the lower layer address outside the IPSec protected domain from where the invoking MAP message came from. There the attacker could read the response in the clear, and use it for attacks.

3.3 The need for a table of MAPSec operation components

A network entity (NE) receiving a MAP message without security header cannot know in general from which PLMN the message was sent. Therefore, the receiving NE cannot make a look-up in the Security Policy Database, which is required according to the current understanding of TS 33.200 v4.0.0 to determine whether the message should have been protected or not. That implies that an attacker would have to simply send unprotected MAP messages without security header to get them always accepted completely defeating the purpose of MAPSec.

A possible solution of this problem is a change in the way incoming messages are handled by the receiving network entity. First of all, the security policy database (SPD) needs to contain a table of MAPSec operation components for incoming messages. MAPSec operation components are operation components which have to be carried in a MAPSec message. i.e. with a MAP security header. When an NE receives a MAP message without security header it first goes to that table. If the operation component in the received MAP message is contained in the table and fallback to unprotected mode is not allowed for messages received from that PLMN then the message is discarded, otherwise it is processed as in MAP without MAPsec. Such a table and the corresponding processing are not yet described in TS 33.20 V4.0.0. The table is necessarily independent of PLMN-Ids because MAP messages without security header do not contain source PLMN-Ids in general. This fact is also in conformance with Req.2 (uniformity of protection profiles) above.

4 Need for Security Relevant Clarifications in Section 6

4.1 Protection Groups

In section 6.2 it is said “This section specifies groups of messages and their protection modes at the operation component level. Individual protection groups or particular combinations of groups can then be used to construct protection profiles as specified in section 6.3.”. In section 6.3 it is said “Protection profiles can be individual protection groups or particular combinations of protection groups. MAP protection profiles are coded as a 16 bit binary number where each bit corresponds to a protection group. Currently only 5 groups are defined, the rest are reserved for future use.”

It is not clear from these formulations whether these protection groups are examples and it is allowed for operators to define other protection groups, or whether only the protection groups defined in this TS may be used until further protection groups are specified in future updates of this TS.

It is **proposed** to allow operators to define other protection groups, but to recommend to only use the protection groups defined in the standard.

Reason: If no other protection groups than those defined in TS 33.200 v4.0.0 are allowed then PLMNs have the choice to either encrypt “send authentication info” or not protect it at all. But it is well known that certain important countries are unlikely to allow encryption. On the other hand, the discussion on the introduction scenario for MAP security which lead to the proposal of a cut-off date showed that, in order to prevent active attacks, it is necessary that at least integrity (protection mode 1) is provided globally, benefiting also those operators who deployed full-strength MAPsec (including protection mode 2).

4.2 Protection Profiles

In section 6.3 it is said “The following protection profiles are defined.“

It is not clear from this formulation whether these protection profiles are examples and it is allowed for operators to define other protection profiles, or whether only the protection profiles defined in this TS may be used until further protection profiles are specified in future updates of this TS.

It is **proposed** to allow operators to define other protection profiles. These become necessary in particular when operators may define new protection groups.

It should be further clarified whether protection profiles are **unidirectional** or whether the same protection profiles are to be applied in both directions. Unidirectional PPs give greater flexibility in the definition of security policies, but bidirectional PPs are simpler.

5 Conclusions

The proposals contained in this document shall be agreed by S3 and implemented in a CR to TS 33.200 v4.0.0 .