3GPP TSG SA WG3 Security S3-000688
Meeting S3#16
Sophia Antipolis, 28-30 November, 2000

Source: Siemens AG

Title: Introduction of MAP security

Document for: Discussion and decision

Work item: Core Network Security

Agenda item: tbd

Abstract

This contribution slightly updates S3z00019. It highlights the weakness of a partial introduction of MAP security and proposes to mandate support of MAP security after a certain cut-off date. The contribution deals only with the security problems arising during the introduction of MAP security, but it should be thoroughly studied whether similar problems may occur in the introduction of other core network security protocols.

1. Introduction

Currently, it seems unlikely that MAP security will be implemented in every PLMN at the same time. Situations where network operators A and B have reached agreement on the use of MAP security, but operators A and C have not, may persist for a long time unless a different way forward is explicitly agree upon. PLMNs are thus divided in two categories, those which support MAP security (also called protected PLMNs here) and those which do not. MAP messages within and between PLMNs of the former category are secured, all other MAP messages are not. The limited value of such a partial introduction of MAP security is shown in section 2 of this contribution. We propose countermeasures in section 3.

For simplicity, we assume that either all nodes in a PLMN support MAP security or none. If this assumption is not true, the situation is expected to become rather worse.

2. Attack Scenarios

The following two assumptions are the **rationale for the introduction of MAP security**:

- MAP messages carry information which, when eavesdropped upon or tampered with by an attacker, may be used by him to cause significant damage;
- it is possible for an attacker to eavesdrop on or tamper with MAP messages with a significant probability.

Significant **threats** which may result from a breach of MAP security include:

- Theft of UMTS authentication vectors (AVs) allows an attacker to mount false base station attacks. The AVs may be obtained anywhere, the false base station attack must be carried out at the actual location of the user. If the intercepted AVs can be replayed to a VLR instead of the genuine response to the VLR’s MAP-SendAuthentication-Info message then the user can be impersonated at that VLR independent of the actual location of the user.
- Manipulation of user controlled input in MAP messages used to change call forwarding addresses allows an attacker

to make fraudulent calls and mount call selling operations at the user’s expense.

We now further distinguish between **the type and the place of an attack** on MAP messages. In passive attacks, an attacker just eavesdrops on messages, in active messages he modifies content of the MAP messages or creates new such messages. The attacker may perform his attack at a node or a link within a protected PLMN or between two protected PLMNs or at some other node or link. There is no obvious reason to assume that only passive attacks should be possible.

We would also like to point out that answering our concerns with the remark that the described attacks are unlikely to occur does not appear legitimate in the context of MAP security, as such an answer would appear to implicitly question the rationale for the introduction of MAP security.

Passive attacks on MAP messages:

Here, any MAP traffic within and between protected PLMNs is not affected by attacks. Passive attacks are only possible on MAP messages with origin or destination in an unprotected PLMN. But unprotected messages may be intercepted not only in unprotected PLMNs, but also in protected PLMNs if the attacker knows how the unprotected messages originating from or destined to an unprotected PLMN are routed within the protected PLMN (or if the attacker happens to hit upon them by chance).

If only passive attacks were possible MAP security would be of potentially significant value for an operator whose PLMN supports it because only users roaming into unprotected PLMNs would be potentially affected by the attacks. Depending on the situation, this could imply that only a small portion of users and of the MAP traffic was affected, reducing the risk.

Active attacks on MAP messages:

But, as we have already said above, there is no obvious reason to assume that only passive attacks should be possible. Active attacks may be carried out in a protected or unprotected UMTS PLMN, or even in a GSM PLMN. The attacker can take advantage of the fact that unprotected MAP messages do not contain information about the addresses of the PLMNs or nodes involved. This address information is only contained in the SCCP layer. If the principle of the separation of layers is followed then no address spoofing by the attacker is necessary because at the MAP layer it cannot be decided on the basis of address information whether the MAP message should be protected or not. But even if address information was available at the MAP layer (e.g. by explicitly introducing it in a post Rel’99 specification or by a proprietary implementation handing this information from the SCCP layer to the MAP layer) this would not be sufficient to prevent this type of attacks. The attacker would then only have to modify the SCCP calling party address.

Case 1: attack in an unprotected UMTS PLMN
The attacker may forge an (unprotected) MAP-SendAuthenticationInfo message to obtain AVs for any user of **any** PLMN, independent of the actual location of that user. The attacker must be able to gain access to the response to the MAP-SendAuthenticationInfo message, e.g. by gaining access to the originating node or to a node or link through which the response message is routed. There is no additional problem for the attacker if address information is available at the MAP layer because he can use the correct sending PLMN address.

Case 2: attack in a protected UMTS PLMN
There is a difference to case 1 only if the attacker must assume that address information is available at the MAP layer. He must then modify this address information so that the MAP message looks as if it was sent from an unprotected PLMN. The attacker must have sufficient knowledge of the routing of such messages that he can attack at links or nodes through which such messages pass.

Case 3: attack in a GSM PLMN
It is possible to send MAP messages which are used to change a call forwarding address for a UMTS user also from GSM networks. The attacker need not be able to intercept a response message, and he can use the true sending PLMN Id.

All these active attacks on users of MAP-protected UMTS PLMNs are possible as long as there are unprotected UMTS or GSM PLMNs which are allowed to communicate with the protected UMTS PLMN, i.e. with which roaming agreements exist. The attacks are independent of the actual location of the user.

3. Countermeasures

In an ideal world, all UMTS and GSM operators would confidentiality and integrity protect there MAP networks using MAP security with protection mode 2. But it is well known that there are important countries which do not allow the use of encryption, so the best one can hope for is the ubiquitous use of MAP security with protection mode 1 (integrity only) and widespread use of MAP security with protection mode 2.

In fact, the requirement that all UMTS and GSM PLMNs support MAP security with protection mode 1 after a certain cut-off date appears to be a minimal requirement if one wants to counter the attacks described in section 2. If only attacks against UMTS authentication vectors are to be countered then, of course, it would be sufficient to mandate only UMTS nodes to support MAP security with protection mode 1.

If this minimal requirement cannot be satisfied then the introduction of MAP security appears to be of quite limited value. If this requirement is satisfied, but if not all operators have introduced also protection mode 2 then only passive attacks will be possible, and the situation is as described in section 2 for this case.

It is also necessary to agree on a list of protected messages. This list may be introduced in two steps to allow for fast introduction: in a first step, only the messages whose interception or modification has the highest fraud potential should be protected, in a second step, the list should be completed to include also messages involving a lower risk.

Conclusion

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 agreement on the cut-off date has to be complemented by the agreement on a list of messages urgently requiring protection. An unprotected message from the list would then be rejected when received from any source after the cut-off date. A second (later) cut-off date after which further, less critical, MAP messages shall be protected may be defined later.

S3 are asked to endorse this proposal and to compile a list of MAP messages urgently requiring protection.

It is proposed that S3 send an LS to the SA plenary asking to endorse a cut-off date for the introduction of MAP security, and to send an appropriate liaison to the GSM association.