3GPP TSG SA WG3 Security — S3#13 **S3-000312**

23-26 May, 2000

Yokohama, Japan

(Ad-hoc meeting on MAP Security, Yokohama, 23 May, 2000)

Source: **Siemens AG**[1]

Title: **Independence of confidentiality and integrity in MAP Layer III and other layer III issues**

Document for: **Discussion and decision**

Agenda Item: **<Ad-hoc MAP Security meeting>**

Abstract

MAP security layer III, as described in 3G TS 33.102 v3.4.0 (UMTS Security Architecture) uses a well-known method to provide integrity using an encryption function and a hash function. In accordance with what is suggested in the literature, it is proposed here to use a MAC-function (keyed hash function) instead of a keyless hash function so as to provide independence of confidentiality and integrity protection. The impacts on message formats and computation efforts are minor. In protection mode 1, the message even gets somewhat shorter. However, separate keys will be needed for confidentiality and for integrity. The current solution uses only one key for the encryption function. We propose to compensate for this by using the same key for both directions, and distinguish the directions by the sending PLMN Id in the integrity-protected part of the message, without a reduction of the security level. This latter proposal is, however, independent of the rest. We also point out open issues to be resolved.

1. Introduction

MAP security layer III, as described in [1] 3G TS 33.102 v3.4.0 (UMTS Security Architecture) uses a well-known method to provide integrity using an encryption function and a hash function. This method has been described and analysed in the literature. We refer to [2, section 9.6.5.] and take up suggestions found there.

The method used in [1] takes two forms, depending on whether integrity alone is required (protection mode 1, described in [1, section 7.4.2.2]) or whether both confidentiality and integrity are required (protection mode 2, described in [1, section 7.4.2.3]).

According to [1, section 7.4.2.2], the message body of Layer III messages in protection mode 1 takes the following form:

Cleartext||TVP||$E_{KSXY(i)}$(*Hash*(MAP Header||Security Header||Cleartext||TVP))

In other words, a message x (consisting of MAP Header||Security Header||Cleartext||TVP) is followed by an integrity check value which is computed as E(*Hash* (x)) where E is an encryption function, giving (x, E(*Hash*(x)). This correponds to [2, 9.86 Remark 1].

According to [1, section 7.4.2.3], the Layer III Message Body in protection mode 2 takes the following form:

$E_{KSXY(i)}$(Cleartext||TVP||*Hash*(MAP Header||Security Header||Cleartext||TVP))

[1] This document is based on work carried out in the EU-sponsored collaborative research project USECA (http://www.useca.freeserve.co.uk/). Nevertheless, only the author is responsible for the views expressed here.

In other words, a message x (consisting of MAP Header||Security Header||Cleartext||TVP) is followed by a hash value *Hash* (x) which is then encrypted with the encryption function E, together with a part x' of the message x,
giving E(x', (*Hash*(x)). This correponds to [2, formula (9.2)].

2. Properties

(1) Clearly, in both protection modes 1 and 2, integrity depends on encryption. The integrity protection is only as strong as the encryption function, and when the use of an encryption function is not possible then also integrity protection is not possible, i.e. not even protection mode 1 is then possible. This is undesirable.

(2) The method used in [1] requires that the hash function be collision-resistant when used with protection mode 1. Otherwise, an attacker could substitute one message for another having the same hash and hence the same integrity check value. Due to the birthday paradoxon, the output of collision-resistant hash functions needs to be twice as long as that of a keyed hash function for the same security level (i.e. chance of finding collisions or forging a MAC respectively).

(3) It is mentioned in [2, 9.86 Remark 1.] that a key K used as for protection mode 1 must be exclusively reserved for this integrity function, and not be used for encryption also. Certain chosen-text attacks are mentioned, but it is not clear how they could be carried out in the context of MAP security as in [1]. However, if there was concern about such an attack then two different keys would be needed anyhow for the method used in [1], one for protection mode 1 and one for protection mode 2.

3. Proposal

It is proposed to choose *Hash* to be a MAC-function *H* (keyed hash function) and to use two different keys, a key KSXY(int) to be used with the MAC-function *H* and a key KSXY(con) to be used with the encryption function E (cf. [2, section 9.6.5 (iii)]. The MAC-function H and the encryption function E should be independent. Clearly, when *H* is a MAC-function then, for protection mode 1, the use of the encryption function becomes superfluous.

It is proposed in addition, to use the same key for both directions, and to include the Sending PLMN Id in the security header which is contained in the integrity-protected part of the message. This makes up for the need for separate integrity and encryption keys, without weakening security. If it was decided to keep the concept of separate keys for each directon this would not affect the rest of the proposed changes.

Including the Sending PLMN Id in the security header is useful anyhow because the receiving entity needs to know the sending entity before being able to decrypt. It is against the principles of protocol design and may create technical problems if the sending entity had to be determined from a lower protocol layer.

We also propose to put the time variant parameter TVP first in the integrity-protected message, in accordance with [1, section 6.5.3]. The TVP does not need to be confidentiality-protected. It does not harm to do it from a security point of view, but there may be a performance penalty: Replayed packets would have to be first decrypted before they could be discarded. It is the task of the initialisation vector, not the TVP, to provide sufficient variety in the initial part of the encrypted message.

Remarks pertaining to data types like OCTET strings etc. are proposed to be removed from the text because they belong in a stage 3 description.

The remark about the compatibility of protection mode 1 with the current MAP protocol is not accurate because of the presence of the security header. It is therefore proposed to remove it.

We therefore propose to replace [1, section 7.4.2.2] with the following:

7.4.2.2 Protection Mode 1

The message body of Layer III messages in protection mode 1 takes the following form:

TVP||Cleartext|| $H_{KSXY(int)}$(TVP|| MAP Header||Security Header||Cleartext) where "Cleartext" is the message body of the original MAP message in cleartext. Therefore, in Protection Mode 1 the Layer III Message Body is a concatenation of the following information elements:

- Time Variant Parameter
- Cleartext
- Integrity Check Value

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function *H* to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and Cleartext.

[Note1: There is need for replay protection of Layer III messages; it is envisaged to use TVP for this purpose. The precise definition of the use of TVP is ffs.]

We propose to replace [1, section 7.4.2.3] with the following:

7.4.2.3 Protection Mode 2

The Layer III Message Body in protection mode 2 takes the following form:

$$\text{TVP}\|\ \text{E}_{\text{KSXY(con)}}(\ \text{Cleartext}\|\ H_{\text{KSXY(int)}}(\text{TVP}\|\ \text{MAP Header}\|\text{Security Header}\|\text{Cleartext}))$$

where "Cleartext" is the original MAP message in cleartext. Message confidentiality is achieved by encrypting cleartext, TVP and integrity check value with the confidentiality session key KSXY(con). Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function *H* to the concatenation of Time Variant Parameter TVP, MAP Header, Security Header and Cleartext.

[Note1: There is need for replay protection of Layer III messages; it is envisaged to use TVP for this purpose. The precise definition of the use of TVP is ffs.]

We propose to replace [1, section 7.4.3] with the following:

7.4.3 Structure of Security Header

The security header is a sequence of the following data elements:

- Protection Mode
- Key Identifier
- Algorithm Identifier
- Mode of Operation
- Initialisation Vector
- Sending PLMN Id

NOTE: Whether the Initialisation Vector is needed depends on the mode of operation of the encryption algorithm.

4. Open issues

The type, length and use of the TVP is tbd. The requirements are not fully clear yet, especially concerning the necessary length to prevent a wrap around and a suitable window size at the receiver. Possible solutions include sequence numbers and windows (e.g. IPSec uses 32 bit sequence numbers and >32 bit windows) or a mix of time-stamps (UTC) and nonces where the nonces are used to distinguish between messages with the same time stamp. (e.g. ITU H.235 uses a 64 bit TVP of this structure.)

Security association for layer III: It is necessary for interoperability to agree on the definition of a security association which has to be negotiated in layer I and transmitted to the network entities in layer II. Parameters will include addresses, keys, protection modes, operation modes and algorithms.

5. Evaluation

Message structure: The overall message structure is preserved. So, the influence on ongoing work in 3GPP CN should be minimal.

Computational effort: A common realisation of a MAC-function is the H-MAC which requires two applications of a hash function H (cf. e.g. [3, 9.67]). In protection mode 1, the additional application of the hash function is compensated for by the fact that encryption need no more be applied. In protection mode 2, an additional application of the hash function would be required indeed if H-MAC was used. The application of hash functions is fast, so this is considered acceptable.

Message lengths: In protection mode 1, the message becomes actually shorter for the reason mentioned in section 2 (2).(A typical value for the saving would be 80 bits.) In protection mode 2, the message length becomes also shorter or remains the same, depending on whether the same or a different hash function was meant to be used in [1] for protection modes 1 and 2.

Key management: When our suggestion is accepted to use the same keys for both directions (together with the inclusion of the Sending PLMN Id in the security header) then the overall length of the key management messages in layers 1 and 2 remains the same. But even if the number of key bits to be established in layer I and transported in layer II would double this would still be considered acceptable given the overhead of the messages in these layers.

Conclusion

The additional effort, if any, caused by our main proposal to separate confidentiality and integrity, is quite small, as shown in section 4. Other disadvantages cannot be seen. The separation of integrity and confidentiality could prove quite useful in certain scenarios not all of which can be foreseen today. The other changes are meant to clarify issues. It is therefore concluded that the proposals made in section 3 should be accepted by 3GPP SA3. The open issues remain to be dealt with.

References

[1] 3G TS 33.102 v3.4.0 (UMTS Security Architecture)

[2] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.