3GPP TSG-SA3 Meeting #15bis
(Ad-hoc on aSIP and NDS WIs)
Munich, 8th – 9th November 2000

S3z000017

Agenda Item: -

Source: Ericsson

Title: Replay Protection for MAP Security

Document for: Discussion and decision

1 Introduction

This contribution proposes a change to the way Replay Protection is currently provided in MAP Security.

In particular, it is proposed to include the Time Variant Parameter (TVP) in the Security Header in order to avoid the extra overheads of the TVP in the protected payload of secure MAP operations. It is also proposed to use the value of the TVP to build the value of the Initialisation Vector (IV).

2 Background

Current definition for Replay protection of core network signalling is based on the use of time-stamps as TVP. TVP is used as part of the integrity protection mechanism to provide replay protection. For example, TVP is used in Protection Mode 1 as follows:

$$\mathbf{TVP}\|\text{Cleartext}\|\ H_{KSXY(int)}(\ \mathbf{TVP}\|\text{Security Header}\|\text{Cleartext})$$

… and in Protection Mode 2:

$$\mathbf{TVP}\|\ E_{KSXY(con)}(\ \text{Cleartext})\ \|\ H_{KSXY(int)}(\mathbf{TVP}\|\text{Security Header}\|\ E_{KSXY(con)}(\ \text{Cleartext}))$$

On the other hand, the use of IVs is proposed to prevent codebook attacks against encrypted traffic. The IV is included in the Security Header and its value shall be different and unique between sending NEs.

3 Combined use of TVP and IV

Since the Security Header is used as part of the integrity protection mechanism, some extra overheads in the protected payload of secure MAP operations could be avoided if TVP is moved to the Security Header and it is not explicitly used as part of the integrity protection mechanism.

The TVP should be the first part of the security header, and the security header should be the first part of the data on which MAC is calculated the to let this “random” quantity influence the calculations right from the beginning. This still provides the same level of protection against replay attacks.

On the other hand, the random value of TVP (time-stamp) in the Security Header could be used to build the IV. Since at the same point of time two NEs could be using the same TVP, it is required to add something to the TVP in order to make the IV unique between two sending NE’s. The idea is to use the NE-address (E.164 vlr/hlr-address) or part of it.

Following these principles, Ericsson proposes the following format for the protected payload of Secure MAP operations and also a definition for the combined TVP/IV parameter in the security header:

> **Note:** This proposal assumes the changes proposed in S3z000013 'General Structure of Secure MAP Operations' and in S3z000015 'Structure of Security Header for MAP Security'.

7.4.2 Format of Secured MAP Message Body

7.4.2.1 Protection Mode 0

Protection Mode 0 offers no protection at all. Therefore, the protected payload in protection mode 0 is identical to the original MAP operation payload in cleartext.

In case Protection Mode 0 is to be used, the mechanism shall also allow to perform the operation in cleartext, thus avoiding the extra load introduced by the Security Header.

7.4.2.2 Protection Mode 1

The protected payload of Secured MAP operations in protection mode 1 takes the following form:

~~TVP||~~Cleartext|| $H_{KSXY(int)}$(~~TVP||~~Security Header||Cleartext)

where "Cleartext" is the payload of the original MAP operation in clear text. Therefore, in Protection Mode 1 the protected payload is a concatenation of the following information elements:

- ~~Time Variant Parameter TVP~~
- Cleartext
- Integrity Check Value

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of Time Variant Parameter TVP, Security Header and Cleartext.

~~The TVP used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.~~

7.4.2.3 Protection Mode 2

The protected payload in protection mode 2 takes the following form:

~~TVP||~~ $E_{KSXY(con)}$(Cleartext) || $H_{KSXY(int)}$(~~TVP||~~ Security Header|| $E_{KSXY(con)}$(Cleartext))

where "Cleartext" is the original MAP operation payload in clear text. Confidentiality is achieved by encrypting Cleartext with the confidentiality session key KS_{XY}(con). Authentication of origin and integrity are achieved by applying the message authentication code (MAC) function H with the integrity session key KS_{XY}(int) to the concatenation of ~~Time Variant Parameter TVP,~~ Security Header and $E_{KSXY(con)}$(Cleartext).

~~The TVP used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.~~

It is further recommended the use of protection mode 2 whenever possible as this makes replay attacks more difficult.

7.4.3 Structure of Security Header

The Security Header is a sequence of the following data elements:

- **Time Variant Parameter / Initialization Vector (TVP/IV):**
  The TVP used for replay protection of Secured MAP operations is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived must be agreed as a system parameter, the size of the time-window at the receiving network entity need not be standardised.

  Initialization vectors are used with block ciphers in chained mode to force an identical plaintext to encrypt to different cipher texts. Using IVs prevents launching a codebook attack against encrypted traffic. The issue is discussed in more detail in RFC 2406. IV has only local significance in the NE.

  When this parameter is used as an IV, the sending NE's address (padded with zeroes to yield the required length) is appended to the TVP value (TVP || NE-address). The length of the TVP/IV should be at least 64 bits.

- **Sending PLMN-Id:**
  PLMN-Id is the ID number of the sending Public Land Mobile Network (PLMN). The value for the PLMN-Id is formed from the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the destination network.

- **Security Parameter Index (SPI):**
  SPI is an arbitrary 32-bit value that is used in combination with the sender's PLMNID to uniquely identify a MAP-SA.

~~□**Initialization Vector (IV):**~~
~~Initialization vectors are used with block ciphers in chained mode to force an identical plaintext to encrypt to different cipher texts. Using IVs prevents launching a codebook attack against encrypted traffic. The issue is discussed in more detail in RFC 2406. IV has only local significance in the NE.~~

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

- **Original Component identifier:**
  Identifies the type of component within the MAP operation that is being securely transported (Operation identified by operation code, Error defined by Error Code or User Information).