3GPP TSG-SA3 Meeting #18
Phoenix, 21st – 24th May 2001

S3-010197

Agenda Item: 9.1

Source: Ericsson

Title: Use of Combined TVP/IV parameter

Document for: Discussion and decision

1 Introduction

This contribution compiles the working assumptions agreed at S3#17bis (ad-hoc session on NDS) during the course of the discussions regarding the use of a combined TVP/IV parameter.

This paper also introduces the changes required to 33.200 in order to incorporate the agreed working assumption into the specification.

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:

TVP||Cleartext|| H(**TVP**||Security Header||Cleartext)

… and in Protection Mode 2:

TVP|| E(Cleartext) || H(**TVP**||Security Header|| E(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 Use of Combined TVP/IV

According to the agreements at S3#17bis, the Time Variant Parameter (TVP) used to provide Replay Protection, shall be included in the Security Header and not explicitly used as part of the integrity protection mechanism. This will avoid some extra overheads introduced by the TVP in the protected payload of secure MAP operations.

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.

Some of the details on the structure of the TVP were also discussed and the following working assumptions were reached:

- Length: 4 octects (32 bits).
- Clock Resolution: 1 second.
- Clock Reference: Absolute time.

It was also agreed that once the TVP in the Security Header, it shall be used to build the value of the Initialisation Vector (IV).

Since at the same point of time two NEs could be using the same TVP, it was required to append additional elements to the TVP:

- **Unique Node-Id:** This Node-Id is required to achieve that different NEs uses different IV values within the same TVP period. It was suggested to let the Node Id be 3 octets long and that it should be constructed by means of a hash function over the E.164 Global Title address of the MAP-NE. All the details of this Node-Id, including the definition of the hash function, shall be further specified.
- **Local Counter:** A local counter is required in order to create different IV values for different MAP protected messages sent within the same TVP period (1 second). It was suggested to let the Local Counter be 1 octet long. The source of such counter shall be further specified.

4 Changes Required to 33.200

Following these working assumptions, Ericsson understanding on the impacts to 33.200 is the following:

5.4 MAPsec structure of protected messages

5.4.1 MAPsec protection modes

MAPsec provides for three different protection modes and these are defined as follows:

Protection Mode 0: No Protection

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, and Authenticity

MAP operation protected by means of MAPsec consists of a Security Header and the Protected Payload. Secured MAP messages have the following structure:

Security Header	Protected Payload

In all three protection modes, the security header is transmitted in cleartext.

In protection mode 2 providing confidentiality, the protected payload is essentially the encrypted payload of the original MAP message (see chapter 5.4.4). For integrity and authenticity in protection modes 1 and 2, the message authentication code is calculated on the security header and the payload of the original MAP message in cleartext and it is included in the protected payload. In protection mode 0 no protection is offered, therefore the protected payload is identical to the payload of the original MAP message.

5.4.2 Protection Mode 0

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

For cases where Protection Mode 0 is to be used the protection level will be identical to the original unprotected MAP message. It is therefore allowed as an implementation option to let Protection Mode 0 operations be sent without the security header.

5.4.3 Protection Mode 1

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

~~TVP~~‖Cleartext‖ H(~~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 key defined by the security association 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 shall 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.~~

5.4.4 Protection Mode 2

The protected payload of Secured MAP Messages in protection mode 2 takes the following form:

~~TVP~~|| E(Cleartext) || H(~~TVP~~||Security Header|| E(Cleartext))

where "Cleartext" is the original MAP message payload in clear text. Confidentiality is achieved by encrypting Cleartext with the confidentiality key defined by the security association. Authentication of origin and integrity are achieved by applying the message authentication code (MAC) function H with the integrity key defined by the security association to the concatenation of ~~Time Variant Parameter TVP,~~ Security Header and encrypted Cleartext.

~~The TVP used for replay protection of Secured MAP messages is a 32-bit time-stamp. The receiving network entity shall accept a message 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 recommended to use protection mode 2 whenever possible as this makes replay attacks even more difficult.

5.5 MAPsec 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.

  NOTE: It is recommended the use of absolute time clock reference and a 1 second clock resolution.

  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, a unique identifier of the NE and a Local Counter shall be appended to the TVP. The structure of the combined TVP/IV parameter will be then as shown below:

  - **TVP:** 4 octects time-stamp used for replay protection.
  - **Unique NE-Id:** 3 octets used to create different IV values for different NEs within the

same TVP period.

NOTE: It has been suggested to constructed this Node Id by means of a hash over the E.164 Global Title address of the NE. All details of the Node-Id, including the definition of the hash function shall be specified.

- **Local Counter:** 1 octect used to create different IV values for different protected MAP messages within the same TVP period.

  NOTE: Details of the Local Counter shall be specified.

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

- **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.

- ~~**Initialisation Vector (IV):**~~

  ~~Initialisation 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 IV has only local significance in the MAP-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).

5 Conclusions

S3 members who were not able to attend the S3#17bis ad-hoc on NDS are kindly asked to comment on the agreed principles for the handling of this combined TVP/IV parameter.

If no major issues are identified, S3 is asked to endorse the working assumptions agreed in Madrid and to incorporate such agreements into 33.200 as proposed in this contribution.

Based on these principles further work should be progressed in order to define:

- Details of the Node-Id (E.164 address, definition of the hash function, input parameters...).
- Details of the Local Counter (source, bit ordering, …).
- Details on the TVP clock (source, bit ordering, …).

Finally, S3 is also asked to inform N4 on this decision since the changes now introduced in 33.200 have a clear effect on the structure of the security header and the protected payload also defined and referred by N4 specifications (29.002).