3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010116**

13 September, 2001

Sophia Antipolis, France

Source: **Hutchison 3G UK**

Title: **Mandate MAPsec vs Protected Message Table**

Document for: **Discussion/Decision**

Agenda Item:

S3z010085 briefly discusses applying MAPsec to all messages but dismisses the idea in favour of using a table stored in the SPD. Both methods can provide the same level of security, but it is suggested that the overhead of applying MAPsec to all messages means the table solution is better. This contribution examines in greater detail the disadvantages of both methods.

The disadvantage of applying MAPsec to all messages is the overhead of the security header in MAP operations that require no protection, in which case the security header can be reduced to 5 bytes.

The disadvantages of using a table in an NE's SPD are not so easy to quantify. Firstly it is necessary to have bi-directional Protection Profiles. It is not clear that this is a disadvantage, except (maybe) for the constraints it puts on SA management. The main disadvantage of the table would seem to be the need to update it as Protection Profiles change. Protection Profiles may change as new MAP operations are standardised, as new security threats are discovered involving currently unprotected MAP messages and as processing power improves and more MAP operations are protected. For a fully automated system, there needs to be an automatic way of upgrading the SPD in each NE as the Protection Profiles change. This seems to add unnecessary level of complexity to MAPsec, as it is not immediately obvious how to update the table in a robust manner.

The choice between these two methods is not a clear one as each method has disadvantages. This contribution proposes applying MAPsec to all messages, as it appears to be a cleaner and easier solution.

Message Flows

This section contains message flows assuming that MAPsec is applied to all messages. The message flows also assume that fallback to unprotected mode on receiving/replying to messages is handled by a global indicator in the SPD, whereas fallback on initiating a message is handled by on a PLMN by PLMN basis and stored either in the SPD or in SAs in the SAD. The Sending PLMN-Id has been removed from the security header. The definition of MAP protected message here is one sent in a MAP security tunnel, regardless whether protection was actually applied.

Sending/Replying NE performs the following

1. IF NEa is responding to an unprotected message, then NEa sends an unprotected message to NEb. Flow ends (this step can be removed if every NE is MAPsec enabled).
2. NEa checks SPD for the policy towards PLMNb.
    a. If policy mandates MAPsec, then goto 3.
    b. If MAPsec not mandated, then an unprotected message is sent. Flow ends.
    c. If no policy, then abort with error.
3. NEa looks for valid SA in SAD towards PLMNb
    a. If no valid SA, then abort with error.
    b. If more than one valid SA, use the one with closest expiry time.
4. Process MAP message according to SA and send it.

A receiving NE performs the following:

5. If unprotected message received, NEb checks the fallback indicator in SPD.
    a. If fallback allowed, then message is processed. Flow ends.
    b. If fallback not allowed, the abort with error.
6. If protected message received, then NEb uses SPI to retrieve SA from SAD.
    a. If SA not valid, then abort with error.
    b. If SA valid, NEb retrieves Sending PLMN-Id.
7. NEb checks SPD with Sending PLMN-Id
    a. If MAPsec not mandated (including no entry), then abort with error.
8. NEb undoes protection and checks TVP and Integrity as necessary.
    a. If TVP or Integrity check fails, then abort with error.
    b. Otherwise the message is processed.