3GPP TSG SA WG3 Security — S3#15 **S3-000564**

12–14 September, 2000.

Washington.

Source: **Motorola**

Title: **Optional Element to Element IPsec**

Document for: **Decision**

Agenda Item:

Proposal

This document proposes to introduce optional network element to network element (NE-NE) core network security using IPsec. This is in addition to network to network security provided at the edge of the network. The reasons for giving this option are:

- Increased granularity of security services.
- Provides end-to-end inter-network signalling security.

AH (that is, message authentication without encryption) can be used to protect the internal network from malicious modification, insertion and replay of messages. If end to end encryption is desired, then ESP can be used.

The architecture proposed to do this is the architecture to maintain full IPsec security services in the 3 layer key distribution architecture. This was introduced in Tdoc412 (attached). Briefly, KACs negotiate IPsec SAs at Layer I and then distribute them to the appropriate NEsat Layer II. The NEs can then communicate using these SAs.

The mechanism is primarily intended for securing GTP messages but can be used for any messages sent over IP.

3GPP TSG SA WG3 Security — S3#14 **S3-000412**

1-4 August, 2000.

Oslo.

Source: **Motorola**

Title: **A method to retain the IPsec full security services in the three layer network domain security architecture**

Document for: **Discussion**

Agenda Item: **tbd**

Introduction

This document addresses how to retain full IPsec security services for GTP and MAP/IP messages secured using IPsec within the three layer core network security model. In particular, we address the problem of providing protection against replay in this context.

The mechanism to provide replay protection in MAP/SS7 is at the MAP layer, so this mechanism will not provide replay protection for GTP. Thus, another mechanism is needed. IPsec replay protection cannot be provided in the three layer security model when only encryption keys are distributed from KAC to NEs nor when key exchange is manual (see discussion below).

Therefore, the proposed solution is to:

1. Use IPsec IKE for Layer I to generate Security Associations (SAs).
2. Distribute whole SAs at Layer II, instead of just encryption keys.

IPsec Replay Protection

IPsec SA negotiation determines keys, algorithms, protocols and a sequence number. The sequence number together with an anti-replay window provides replay protection. The anti-replay mechanism is only provided for the entities which negotiated the SA. In the three layer model, it is the KAC of each network which negotiates the SA, the other NEs play no part in the SA negotiation process. This SA is wasted since the KACs do not communicate other than to perform Layer I negotiation.

Replay protection can be maintained only if the keys are distributed automatically (that is, by IKE) because there is a danger that the sequence number could cycle back to 0, which is forbidden in IPsec. With automatic key distribution, SA negotiation can be triggered when the sequence number gets close to cycling (it cycles at 2^{32}). Hence IKE to generate NE SAs, rather than manual key distribution, should be used. It is specified in IPsec RFCs that replay protection SHOULD NOT be provided with manual key distribution.

Performing IKE SA negotiation between NEs directly has two major drawbacks. Firstly, it requires that NEs have the capability to generate Diffie-Hellman keys. Secondly, it generates a lot of traffic, even if the key has already been negotiated by KACs at Layer I. Therefore it is more efficient to perform IKE SA negotiation between KACs at Layer I and proceed as detailed below.

Solution

The proposed solution to providing replay protection on messages secured using IPsec is to distribute whole SAs to NEs instead of just encryption keys. This enables replay protection to be provided without altering the GTP, IP or IPsec message formats. The solution will work for all messages sent over IP, specifically, MAP/IP messages.

The SAs established between the two KACs should contain information about the NEs which require IPsec protection for the communication. Each NE in network X will be sent one SA for each NE in network Y which it communicates with. The IPsec SA will contain the NE addresses as its identifier. This can be done by configuring KAC as client and server side negotiator.)

Event triggers are needed:

- In the KAC to distribute SAs at Layer II after Layer I SA negotiation.
- In each NE to tell the KAC to renegotiate the SA when sequence number cycling is imminent.

The use of a sequence number for each sending network entity in providing protection against replay for MAP messages was discussed and rejected at the Yokohama meeting. The reason for rejecting it was added complexity in the NEs (see Section 2.1 of S3-000368). However, the situation is different for GTP. Our solution provides security at the IP layer and has the simplicity of being able to implement IPsec “out of the box” without having to alter IP, IPsec or GTP message formats.