3GPP TSG SA WG3 Security — S3#15 **S3-000559**

12-14 September, 2000

Washington D.C., USA

Source: Siemens AG

Title: Core network security protocol architecture

Document for: Discussion and decision

Work item: Core network security

Agenda item: tbd

Abstract

This contribution further elaborates on the conclusions of the Siemens-contribution S3-000444 presented at S3#14 and takes into account other contributions presented at S3#14. For a rationale of the conclusions, please refer to S3-000444. This document proposes a core network protocol security architecture that offers interoperable security for MAP/CAP based on either IP or SS7 transport. For native IP protocols, an architecture for IPsec based on security gateways (SEG) is proposed, that allows a flexible realization of the UMTS IP network. Text is proposed for eventual inclusion in the standards.

1. Introduction

In the Siemens contribution S3-000444, we proposed **choices for the security protocols** which are used to secure MAP, CAP and so-called native IP-based protocols. The conclusion was that **MAP and CAP** shall be secured at the **application layer**, irrespective of the transport stack used, and that **native IP-based protocols** shall be secured using **IPSec**.

In Ericssons contribution S3-000434 the concept of **Security Gateways** was proposed. This concept is supported here in principle. However, we propose that the internal structure of the **De-Militarized Zone** (or extranet, as it is called in the revised version of S3-000434), which includes firewalls and possibly other functional entities such as application layer proxies, is **not standardized**. The configuration of such a De-Militarized Zone should be left to each operator. In particular, it should not be standardised by 3GPP whether there are inner and outer firewalls and whether these perform stateful or stateless inspection etc.

We propose to include the text of the following section 2 in the appropriate chapter on “Core network security protocols” in a permanent document which is to be maintained on this work item. This text is meant to be eventually included in the 3GPP specification handling core network security.

2. Proposed text on “Core network security protocols”

Core network security protocols provide security for application layer protocols over interfaces between nodes in the core network. The transport for these application layer protocols is either based on SS7 or on IP. A distinction is made between so-called “legacy” protocols and “native IP-based” protocols. Legacy protocols are application layer protocols which are specified to be used with SS7-based transport. Examples are MAP and CAP over SS7. Legacy protocols may also use IP-based transport. Examples are MAP and CAP over IP. Native IP-based protocols may only use IP-based transport. Examples are GTP or SIP. For legacy protocols, interworking between SS7-based transport and IP-based transport may be required. A corresponding requirement does not exist for native IP-based protocols. Therefore, the two types of protocols are handled separately in the following.

2.1 Security for legacy protocols

For legacy protocols, network entities must be able to provide security at the application layer. For legacy protocols over IP, network entities may additionally be able to provide security at the network layer, using IPSec.

If the transport for a run of a legacy protocol is based on SS7 or on a combination of SS7 and IP then security shall be provided at the application layer. If the transport for a run of a legacy protocol is based on IP only then security may be provided at the network layer exclusively or in addition to security at the application layer.

For MAP, security at the application layer shall be provided by the MAP security protocol which is specified in [document/section](tba).
For CAP, security at the application layer shall be provided by the CAP security protocol which is specified in [document/section](tba).

It is ffs whether other legacy protocols need to be considered.

2.2 Security for native IP-based protocols

For native IP-based protocols, security shall be provided at the network layer. The security protocol to be used at the network layer is IPSec as specified in [IETF, rfc2402(AH), rfc2406(ESP)]. All network entities supporting native IP-based protocols must support IPSec.

Note, that IPsec does not support the use of a single SA for hosts with multiple (a list of) IP addresses. Therefore care has to be taken while setting up GTP security where GSN nodes can have multiple IP addresses, or SCTP which offers support for multihomed hosts.

Key management for IPsec shall be automated to support IPsec replay protection.

2.2.1 Security gateways

In order to support security for native IP-based protocols, a special type of network entities (NEs), called Security Gateway (SEG) entities, is defined. These entities shall offer the following functionality:

- SEGs operate at the border of a network, providing IP security for IP communication between different networks.
- SEGs shall be able to establish and maintain IPsec tunnels with any NE of their own network that use this SEG to secure IP traffic to different networks.
- SEGs must be able to establish and maintain IPsec tunnels with SEGs of other networks in order to secure IP traffic between networks. In particular, SEGs must be able to determine the IP address of an appropriate SEG of the destination network.
- SEGs must be able to let specific traffic which need not be secured by the SEG bypass the security functionality.
- SEGs must interoperate with the network's firewalls to provide a maximum level of overall network security.
- An SEG must provide an interface to the entity providing the key management functionality

The key management functionality is logically separate from that of an SEG.

2.2.2 Security endpoints

In order to provide security for native IP-based protocols between network entities in the same network, an IPSec security assocation shall be established between these network entities.

In order to provide security for native IP-based protocols between network entities in different networks, there are two options:

- The endpoints of the IPSec security association coincide with the source and destination IP-addresses determined by the native IP-based protocol (“end-to-end IP security”);
- The IP packets are routed via two Security Gateways, one in the originating network and one in the terminating network which terminate the IPSec security associations (“hop-by-hop IP security”)

For secure IP traffic between network entities in different networks, **hop-by-hop IP security** shall be supported. This requires the originating NE to establish an IPsec tunnel to an appropriate SEG in the same network. The SEG terminates this tunnel and sends the data through another IPsec tunnel between the originating and the receiving network. This second tunnel is terminated by a second SEG, which in turn uses IPsec to pass the data to its final destination (path *a* in figure 1).

End-to-end IP security may be supported. This implies that an IPsec security association is established end-to-end between these NEs (path *b* in figure 1).

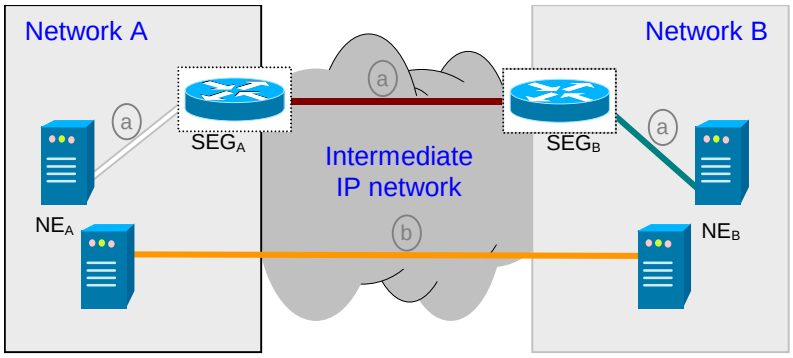

Figure 1: Options for secure IP communication between different networks

2.2.3 Security profiles

For each native IP-based protocol, profiles for the use of IPSec are specified. These may differ for different interfaces or may be identical. A security profile is a selection of options for the use of IPSec in the UMTS core network. When defining security policies and security associations for the use of IPSec [cf. IETF, rfc2401], the options selected in the security profile shall be used, thus reducing the IPSec configurations which need to be supported by the UMTS core network. A security profile need not completely determine the choice of security policies and security associations.

A security profile selects options for the following items:

- Security features: no security or integrity or integrity and confidentiality
- Security endpoint: end-to-end or hop-by-hop or both (cf. section 2.2.2)
- Security protocol: AH or ESP
- Mode: tunnel or transport mode
- Security mechanisms: a set of cryptographic algorithms which must be supported
- Selectors: the selectors which shall be used for security associations
- Mechanism for replay protection
- Support for SA lifetime handling
- Combination of security associations (if applicable)
- Failure handling
- Others [ffs]

2.2.4 Mechanisms for replay protection

Depending on the key management mechanism employed (cf. [document/section](tba)) the replay protection mechanism standardised for IPSec may not be available. In this case, a separate mechanism is specified here:

[tba, use S3-000412 (Motorola) as a basis]

3. Conclusion

The following has been proposed in this contribution:

- For legacy protocols, security shall be provided at the application layer;
- For native IP-based protocols, security shall be provided at the network layer. The security protocol to be used at the network layer is IPSec as specified in [IETF, rfc2402(AH), rfc2406(ESP)]. All network entities supporting native IP-based protocols must support IPSec.
- In order to support security for native IP-based protocols, a special type of network entities (NEs), called Security Gateway (SEG) entities is defined.
- The key management functionality is logically separate from that of a Security Gateway.
- For secure IP traffic between network entities in different networks, hop-by-hop IP security shall be supported. End-to-end IP security may be supported.
- The internal structure of the De-Militarized Zone (Extranet respectively, cf. S3-000434) shall not be standardized.
- It is proposed to standardise security profiles for the use of IPSec in UMTS which limit the variability allowed by the IPSec standard.

Furthermore, it is proposed to include the text of section 2 in the permanent document which is to be maintained on this work item. This text is meant to be eventually in the 3GPP specification handling core network security.