3GPP TSG SA WG3 Security — S3#14 **S3-000444**

2-4 August, 2000

Oslo, Norway

Source: Siemens AG[1]

Title: Core network security protocols

Document for: Discussion and decision

Work item: Core network security

Agenda item: tbd

Abstract

For Release 2000, core network security is required. The paper describes different approaches to secure core network protocols and discusses the advantages and disadvantages of the different approaches. The paper proposes that security for protocols which can be based on both SS7- and IP-transport, such as MAP and CAP, security shall be provided at the application layer for ease of interworking. For "native" IP-based protocols such as GTP or SIP, the use of IPSec should be the working assumption.

1. Introduction

Starting from Release '00, transport in a UMTS core network may be either based on SS7 or on IP. Therefore, in the medium term, will have to consider entities in the UMTS core network supporting the following protocol stacks:

- MAP/CAP over SS7 (for short: MAPo/SS7)
- MAP/CAP over IP (for short: MAPo/IP)
- Application protocols over IP transport with no equivalent protocol over SS7 transport. (for short: native IP-based protocols).

It may well happen that a single platform communicates over both SS7 and IP, e.g. the HSS. Examples for the nodes supporting only native IP-based protocols include the CSCF.

It is not clear whether SS7-based protocols other than MAP/CAP have to be considered here and, if yes, whether they would make any difference to our considerations.

Furthermore, core network security can be provided at the application layer or at a lower layer. If security is provided at the application layer we denote this by application layer security . If security is provided at the IP layer by IPsec [5], we use the term IP security.

[1] This document is partly based on work carried out in the EU-sponsored collaborative research project USECA (http://www.useca.freeserve.co.uk/). Nevertheless, only the author is responsible for the views expressed here.

The following (necessarily symmetric) matrix shows which type of network entity needs to communicate with which other type in the medium term:

	MAPo/SS7	MAPo/IP	native IP
MAPo/SS7	yes	yes	no
MAPo/IP	yes	yes	no
native IP	no	no	yes

2. Security for MAP and CAP

We mention only MAP in the sequel. The same arguments apply to CAP which we do not explicitly mention here.

It is assumed here that, for a long period after the introduction of IP as the transport for MAP, MAPo/IP nodes (e.g. VLRs in network 1) need to be able to communicate with MAPo/SS7 nodes (e.g. HLRs in network 2).

For MAPo/IP security, there are basically two options: Security on the MAP application layer, or IP security. If IP security is used, the need for application-to-network layer security gateways (ANLSG) arises when interworking between IP and SS7 transport becomes neccessary. Such an application-to-network layer gateway would have to translate application layer MAP security (in the SS7 domain) into network layer security (in the IP domain). This is undesirable for several reasons:

- There is additional complexity introduced by such a gateway for which no precedent is known.
- To receive protected MAP messages and to transform them into IPsec secured messages, a SS7/IP gateway must be capable of terminating application layer (MAP) security on the SS7 side. Since MAP routing is based on the IMSI number and does not happen at the MAP-layer, an SS7 end-entity cannot directly address (and usually does not even know) gateways at the network layer or other MAP entities. Therefore, it seems to be difficult to set up a MAP security association betwenn a MAP end-entity and a ANLSG.
- The trust issues raised by this solution are difficult. The endpoints of the MAP communication would have to trust the ANLSG. But how can a MAP/SS7 node even know, which gateway the MAP messages pass? ANLSGs could even be located in intermediate networks, e.g. if the originating network has no direct link to the IP world. So ANLSGs were likely to influence and even restrict the world-wide PLMN topology, for guaranteeing a closed chain of trust between all communicating MAP entities.
- An ANLSG would seem to contradict the principle of a separation between transport stack and application.

This speaks in favour of providing security at the application layer also for MAPo/IP

An additional advantage of this approach is that no additional specification and implementation effort is needed for MAP security when IP-based transport for MAP is introduced.

Therefore, it is proposed that for MAPo/IP nodes and CAPo/IP nodes, security shall be provided at the application layer.

3. Security of native IP-based protocols

For native IP-based protocols security can be applied at the application layer, at the transport layer or at the network layer. The use of IPSec is the only plausible choice for security at the network layer (for short: IP security).

Network layer security has a definite advantage over the other two solutions since it offers a unified solution for all native IP-based protocols in the core network. Application layer security would necessitate approaches specific for each application protocol, and transport layer security is available only for TCP.

A disavantage of IP security is that it may necessitate network layer security gateways, depending on the protocol under consideration. To give an example, a CSCF will, in general, not know the IP address of the HSS on which the data for a particular user can be found. Rather, depending on the routing and addressing schemes for the IM domain, IP addresses will have to be translated by appropriate gateways along the path between CSCF and HSS. But then also IPSec connections have to terminate at such gateway, i.e. these gateways will also have to assume the role of network layer security gateways.

More generally speaking, IPsec can be used in a hop-by-hop or in an end-to-end fashion. The choice between these options clearly depends on the given scenario. In the UMTS R'00 core network, for securing an IP-based protocol end-to-end, end-to-end IP-addressing at the network layer must be done. If hop-by-hop protection is provided all intermediate nodes in the message path will have to be trusted by the end nodes.

End-to-end security based on IPsec between different networks can cause problems with firewalls or NAT (network address translation), e.g. authentication is not possible when authenticated transport information changes in a NAT device, or packets are dropped when a firewall cannot read data elements in encrypted packets. A solution to this problem can be to include security gateways in the NAT devices of firewalls, which terminate a security association on one side and set up a second security association on the other side, and to establish secure tunnels between gateways of different networks.

These issues need careful study. It is unlikely that they can be solved before the routing and addressing schemes for the protocols to be protected are known. But several observations may help here:

- network layer security gateways may be built with standard IP-techniques;
- the trust issue appears solvable if there is a security gateway in each domain of trust (e.g. a PLMN), and if the security gateway in the domain of origin can address and establish a security association with the security gateway in the destination domain at the network layer.

This makes us believe (with all caution) that these issues can be solved and leads us to propose that the provision of security at the network layer should be the working assumption for native IP-based protocols.

4. GTP security

The issues raised in section 3 may be easier to solve for some protocols than for others. A protocol which seems amenable to a (relatively) straightforward solution is GTP. GSNs can address each other directly at the IP layer. There is no IP address translation in between. However, there may be firewalls in between.

IPsec appears to be the most suitable security solution for GTP, in line with what was said in section 3. However, before a decision can be taken two problems which have been raised in [6] need to be solved:

- the role of firewalls is reduced to IP-address filtering. Does this offer sufficient protection?
- depending on the choice for key management, the replay protection mechanism provided by IPSec may not be available.

5. Conclusion and open issues

The following is proposed:

- for MAP and CAP, security shall be provided at the application layer, irrespective of the transport stack used;.
- for native IP-based protocols, the working assumption is to use IPsec.

If these proposals are accepted, several issues remain to be solved. Among them are:

- for the general case of native IP-based protocols, the gateway issues related to routing and addressing, firewalls and NAT have to be solved;
- for GTP, the problems of reducing the role of firewalls to IP-address filtering and of replay protection have to be solved;
- it needs to be determined whether SS7-based protocols other than MAP/CAP have to be considered here and, if yes, whether they would make any difference to our considerations in this document.

References

[1] 3G TS 33.102 v3.4.0 (UMTS Security Architecture)

[2] IETF RFC 2402 : IP Authentication Header (AH)

[3] IETF RFC 2406 : IP Encrypting Security Payload (ESP)

[4] IETF RFC 2409 : The Internet Key Exchange (IKE)

[5] IETF RFC 2401 : Security Architecture for the Internet Protocol

[6] 3GPP NP-000203 “Peer entity authentication and key distribution in supporting UMTS inter-network security“, Motorola, June 2000