TSG-SA WG3 (Security) meeting #15
Washington, September 12 – 15, 2000

S3-0005~~xx~~63

Agenda Item: Network Domain Security

Source: Ericsson

Title: The security architecture

Document for: Discussion and Decision

1 Introduction

The Ericsson contribution S3-000434 was agreed to form the basis for the current working assumption of S3 concerning the security architecture of an IP based system like the one introduced within the release 00 of 3GPP specifications.

This contribution clarifys some issues of that T-doc and details somewhat further the outline of the security architecture.

2 The Security Architecture

2.1 The inter-network security architecture

At the last S3-plenary it was agreed that a new entity called Security Gateway was introduced. Later it has been found that the natural acronym of this entity, SGW, already is commonly used to denote an entity called Signalling Gateway. Due to this ambiguity of the acronym Ericsson therefore proposes to change the name to Network Security Gateway, abbreviated NSG.

The NSG is defined as a security entity located at the network border with the task to enforce the security policies, defined by the operator, concerning the packet flows between the own network and other networks. It can also be used to apply protection to packets exchanged directly with an external host, server or terminal if this is allowed by the policies. ~~It should be clarified, though, that the policies defined in the NSG only apply to packet flows terminated in the network. In this respect UEs should be considered attached to, but not part of, the network.~~
Ericsson envision that sensitive application level data - be it authentication data sent between the user and a service domain, a banking transaction, or any other sensitive data – will, and should, be protected using application level security mechanisms, since the trust relation in action is between the user and the application provider.
This means that ~~“user data”~~data belonging to the user plane, i.e. packet flows over the Gi interface, will not be protected by the ~~network~~ NSG~~.~~, while all data belonging to the control plane will be protected by the NSG according to the relevant policies.

It is recommended that the NSG is placed in a network, a so called Extranet, which is separated from the internal network by a Firewall, FW. Typically also other network elements, like e.g. DNS servers and different types of proxies, could be located in such an Extranet. It is therefore also recommended to protect the Extranet itself by placing a second, outer Firewall between the Extranet and an external, shared transport network.

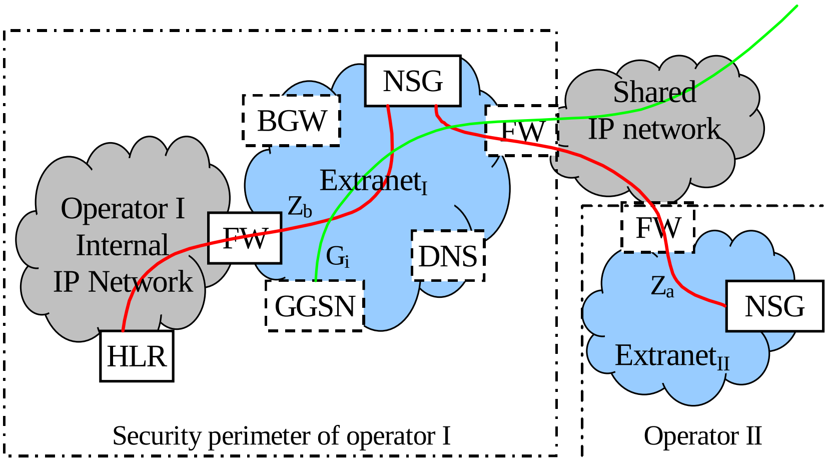

Fig. 1 An example security architecture

Ericsson propose that the NSG should be considered an entity evolved from the Key Administration Center, KAC, previously introduced (see S3-000432) to handle the key management procedures needed for secure MAP communications. With this in mind one is able to destinguish two~~hree~~ separate functional blocks of the NSG:

1. The inherited KAC as being defined in TR 33.xxx. This block is responsible for negotiation, establishment and maintenance of Security Associations, SAs, valid for the node-to-node MAP message protection mechanism.

2. ~~An IKE/IPsec based security mechanism used to protect the “internal” distribution of valid MAP-SAs from the KAC to the different network elements. See TR 33.xxx for more information.~~A second IKE/IPsec compliant security mechanism (defined in IETF RFCs 2401-2409).
This block is responsible for the negotiation, establishment and maintenance of different “external” SAs. There can be more than one SA set up towards any specific network. If allowed by the operator defined policies, SAs might also be setup directly towards external hosts, servers or terminals.

~~A second IKE/IPsec compliant security mechanism (defined in IETF RFCs 2401-2409).~~.

~~One of the reasons to introduce the NSG was to enable an independent choice of security strategy for the internal network. It gets ever more common, though, for operators to build their networks with equipment from multiple vendors. This will require the intra-network security functions of different vendors to be compatible, i.e. there is a need to define a security mechanism mandatory to support for all typical multi-vendor interfaces (e.g. the Iu interface).~~

~~Ericsson therefore propose that IPsec should be mandatory to support for such interfaces.~~

2.2 The intra-network security architecture

As stated in the previous contribution (S3-000434) Ericsson believes that the choice of strategy for the protection of the internal network should be possible to make independantly by each operator. This means that no mechanisms, in this context, should be standardized as mandatory.

Considering that IPv6 seams likely to be chosen, not only to be used for UEs but also for network elements, and the fact that IPsec support is mandatory for all IPv6 implementations, it seams reasonable to introduce IPsec as one optional way to secure a network internally.

In such a scenario it is recommended to place an entity responsible for IPsec termination on the inside of the inner firewall. This would cause the inter-network traffic (still only the packets belonging to the control plane, as mentioned previously) to cross the firewall in clear, enabling that firewall to work in a stateful inspection mode or even as an Application Level Gateway (ALG) if so desired.

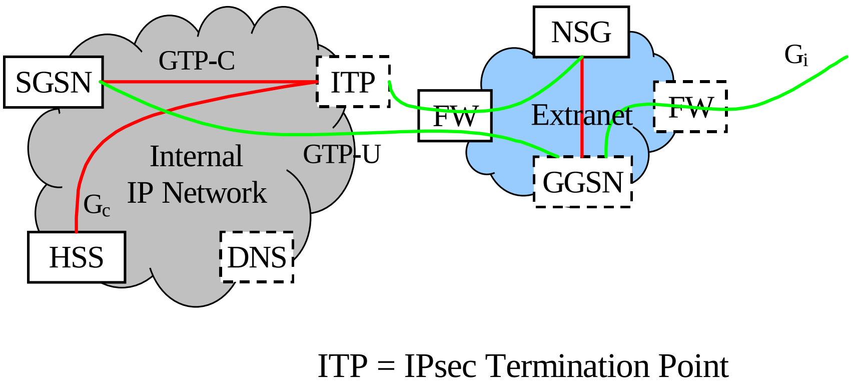

Fig. 2 An example on intra-network security (PS domain)

3 Conclusions

In this contribution Ericsson proposes:

1. To change the name of the previously introduced entity, the Security Gateway, to Network Security Gateway, NSG.

2. To make the outer firewall, as well as the concept of an Extranet, optional, though recommended, to implement.

3. To exclude user traffic (i.e. packets sent over the Gi interface) from the transport level protection mechanisms enforced by the NSG.

4. ~~To make support of IPsec based security mandatory for all intra-network multi-vendor interfaces.~~ To introduce IPsec as one optional way to secure intra-network communications.