3GPP TSG SA WG3 Security S3z000021
Ad-hoc meeting S3#15bis
Munich, 8-9 November, 2000

Source: Siemens AG

Title: SA negotiation protocol for the Z_A interface

Document for: Discussion

Work item: Network domain security

Agenda item: tbd

Abstract

For the Release 5 core network security key management architecture, two different methods were discussed in S3-000445 for negotiating SAs over Z_A to protect security protocols over Z_C between different networks.

The first method is to use IKE (IETF RFC 2409) for SA negotiation directly, the second possibility is to define within 3GPP a new SA negotiation protocol for Z_A protected by IPSec. This contribution discusses the feasibility of the former method focussing on the configuration information which needs to be exchanged during SA negotiation, e.g. IP addresses of the NEs that will use the negotiated SAs to protect their Z_C communication. The contribution concludes that this method is problematic, and outlines an alternative approach. Because it is very desirable that the same procedure for negotating security associations over Z_A is used for all UTMS core network security protocols our contribution also implies that defining a new DOI for MAPSec may not be the right approach.

1 Introduction

By now it is not clear whether IKE can be used for negotiating IPsec SAs (using the IPsec DOI, IETF RFC 2407) directly over the Z_A interface. In this case the core network key management architecture would mean to run the IKE protocol between the KACs of two networks and to run the IPsec kernel (AH, ESP) between (different) NEs. Such a functional split is not intended by the IPsec framework which assumes IKE and the IPsec kernel to operate on the same host, i.e. the same IP address.

Although having IKE and the IPsec kernel on different hosts is an implementation issue as well, it still has further consequences. To discuss this, we first collect some minimal requirements for negotiated configuration information between the KACs and then list the possibilities to distribute this data within an IKE exchange. The problem is that IKE has only limited capabilities to negotiate such configuration data.

In this contribution we use the term NE (network element) for all core network IP entities, including SEG entities (security gateways). Networks that support roaming from one to the other network and therefore require SA negotiation over Z_A between their KAC entities are called „adjacent“.

2 Configuration data negotiated between KAC entities

For determining the minimal amount of data that is required in both KACs of adjacent networks for SA negotiation using the IPsec DOI, it must be determined what data the KACs need to distribute the

resulting SAs in their networks (i.e. to send them to the approporiate NEs and supply them with the required selectors, like IP addresses, ports and protocol type). This surely depends on the granularity of the supported network structure.

- A network configuration supporting at most one IPsec secured channel between two adjacent networks, between two IP addresses known by both sides in advance (that are likely to describe SEGs in this case) is not regarded as sufficient. Only this configuration would not require the exchange of additional information during SA negotiation between the KACs.
- A more realistic assumption is that in each of two adjacent networks there are several NEs that require a secure channel with the other network. One specific NE can have IPsec channels to different NEs of the other network. (example: secure GTP between a GGSN and several SGSNs). **Therefore it is seen as a minimal requirement that the KAC initiating an IKE exchange communicates at least the (source) IP address of the NE in the same network and the (destination) IP address of the NE in the other KAC's network during SA negotiation**. Otherwise the responding KAC would not be able to determine the NE in the responding network the SAs have been negotiated for (it is not sufficient for the initiating network to only send the IP address of the initiating network's NE, since this NE could be configured for secure channels to several destination IP addresses in the responding network).
- It is likely that the configuration information to be exchanged during an IKE SA negotiation over Z_A is more complex than only the source and destination IP addresses of the NEs that receive these SAs. Consider the case that these NEs are SEGs that establish an IPsec tunnel. The operators could require the SEGs to open this tunnel only for two specific groups of end-entities behind the SEGs, one in each network. This would require to not only exchange the SEG's IP addresses but the end-entities' IP-addresses or subnet mask between the KACs during SA negotiation as well.

Since it is difficult to determine the exact configuration requirements for future UMTS IP networks, we propose to use a mechanism for SA negotiation over Z_A that does not limit the flexibility of adjacent networks to establish secure channels between their NEs.

3 Exchanging configuration data within IKE

IKE operates in two phases. In Phase 1 the IKE peers establish a secure channel between themselves. IKE Phase 2 (quick mode) then can be repeatedly executed to negotiate SAs for IPsec. With standard IKE the IKE peers know each other's IP address after Phase 1 negotiation. Since in the UMTS core network these are the KAC IP addresses, additional means are required to transport at least the IP addresses of the two NEs receiving these SAs from the initiating to the responding KAC.

For exchanging more than the IP addresses of the IKE peers, quick mode allows two additional ID payloads to be added to the exchange (called IKE client mode). These ID payloads allow one additional selector for each peer. IKE client mode is originally meant to specify end entities behind IPsec tunnels. The data that can be contained within an ID payload is specified in the IPsec DOI and includes (among others) single IP addresses, ranges of IP addresses and subnet masks. Since only a single ID payload per KAC is allowed to be added within client mode, it is not possible to send two arbitrary IP addresses, which is seen as a minimal requirement for IPsec SA negotiation over Z_A (discussed in chapter 2).

Therefore, we do not regard standard IKE as sufficient for IPsec SA negotiation over ZA.

An approach to negotiate arbitrarily complex configuration data within an IKE exchange between two KACs is to define configuration profiles between two adjacent networks in advance, including all required configuration information for a single IPsec channel, and then exchange a pointer to the according profile when SAs are negotiated. Independent of the mechanism for exchanging profile pointers, the profiles must be exchanged offline between adjacent networks before the KACs can start to negotiate SAs. A change in one network's configuration therefore is likely to require a change in all adjacent network's related configuration profiles.The profiles would have to capture the information for all potential communication partners. This appears very inflexible. Nevertheless, we continue to briefly discuss the implications of such an approach:

An idea to exchange such a profile pointer between two IKE peers or KACs is, again, to use the optional ID payloads in a quick mode exchange. The initiating KAC could use its payload (IDci) to send the pointer to the configuration profile it tries to negotiate the SA for.

The allowed types of ID payload are specified by the IPsec DOI. Although these are capable of transporting a profile pointer or name in principle, the usage of each ID type is specified in the IPsec DOI and using any ID type for a generic profile pointer would conflict with the IPsec specification, as it would mean at least some misuse of quick mode. Furthermore it must be ensured that the ID type chosen for the profile pointer is not evaluated by the IKE implementation itself, which would probably result in errors. It is not clear whether standard-conformant IKE implementations can be used or not.

Before considering such an approach for UMTS core network key management it has to be shown that the approach is technically feasible. A use of IKE that conflicts with the IKE specification should be avoided.

Another approach to carry configuration information within IKE that is mentioned in IETF RFC 2407 is to use certificates for IKE authentication which include information for local policy decision. Here, a basic difference to using quick mode ID payloads is that certificates are used for authenticating an IKE phase 1 exchange. Binding phase 1 to a specific configuration profile described in the certificate, would limit IKE phase 2 (quick mode) to only establish SAs for exactly this profile. If SAs for a different profile shall be established afterwards, a new IKE phase 1 negotiation is required. Since IKE phase 1 based on public key mechanisms is a timeconsuming process, this approach does not seem to be feasible.

4 An alternative approach

The approach discussed in the above chapters, to negotiate IPsec SAs for Z_C directly with IKE seems to be problematic and should only be used for core network key management when its feasibility can be clearly shown and when the solution does not conflict with the IKE specifications.

The above analysis seems to suggest that this may be difficult to achieve. We therefore propose to investigate an alternative approach for SA negotiation over Z_A .

This alternative approach is outlined as follows.

- IKE negotiates IPsec SAs between the KACs for use by the KACs
- With these SAs a channel secured by IPsec is established between the KACs, which is integrity protected, encrypted and offers replay protection.
- This secure channel must be established only once (except key refresh) and is subsequently used to secure the messages of an SA negotiation protocol which is still to be defined.

Such an SA negotiation protocol could consist in an exchange of two (or three) messages:

- The initiating KAC sends an “SA proposal“;
- The responding KAC selects the options in the SA proposal and sends an according “SA confirmation“ to the initiating KAC.
- It is for further study whether a confirmation sent by the initiating KAC to the responding KAC is required.

The information elements and formats of the messages “SA proposal“ and “SA confirmation“ need to be defined. Further issues are the key agreement method which will be largely determined by the question whether joint key control is an issue or not.

5 Conclusions and proposals

Since it is difficult to determine the exact configuration requirements for future UMTS IP networks, we propose to use a mechanism for SA negotiation over Z_A that does not limit the flexibility of adjacent networks to establish secure channels between their NEs. Furthermore, the mechanisms should not conflict with the IKE specifications.

The above analysis seems to suggest that this may be difficult to achieve if IPsec SAs for Z_C are negotiated directly using IKE between the KACs. We therefore propose to follow the alternative approach outlined in section 4.

It is very desirable that the same procedure for negotating security associations over Z_A is used for all UTMS core network security protocols, including MAPSec. This implies that negotiating MAP security associations by using IKE and a newly defined MAPSec DOI may not be the right approach.