3GPP TSG SA WG3 Security — S3#17bis **S3n010012**
23rd April – 24th April
Madrid, Spain

Agenda Item: 7.3 – NDS Session
Source: Ericsson
Title: IPsec and IKE profile for network domain security
Document for: Discussion and decision

1 Scope and objectives

The main objective of this document is to propose additions to the profile according to which IPsec and IKE shall be used in the 3GPP network domain security architecture. This profile is used in four different contexts:

- KAC-KAC communication (IKE)
- KAC-NE communication (IKE, IPsec)
- SEG-SEG communication (IKE, IPsec)
- SEG-NE communication (IKE, IPsec)

The main proposals in this document include the following:

- Multiple limitations in what KAC has to support from IKE.
- Limitations in other uses of IKE: mandatory authentication methods and modes in to be preshared secrets and aggressive mode
- Requiring only IPv6-based IPsec/IKE.
- Limitations in what kind of policies and selectors have to be supported by IPsec.

We also present a few open questions in the profiles, and give tentative answers to them.

2 Introduction

The proposed architecture for the next releases of UMTS includes the use of MAPsec to protect MAP signalling traffic at application layer (see Figure 1), and IPsec to protect other, IP signalling communications (see Figure 2).

MAPsec uses a variation of IKE to negotiate Security Associations which is also a part of the IPsec protocol set.

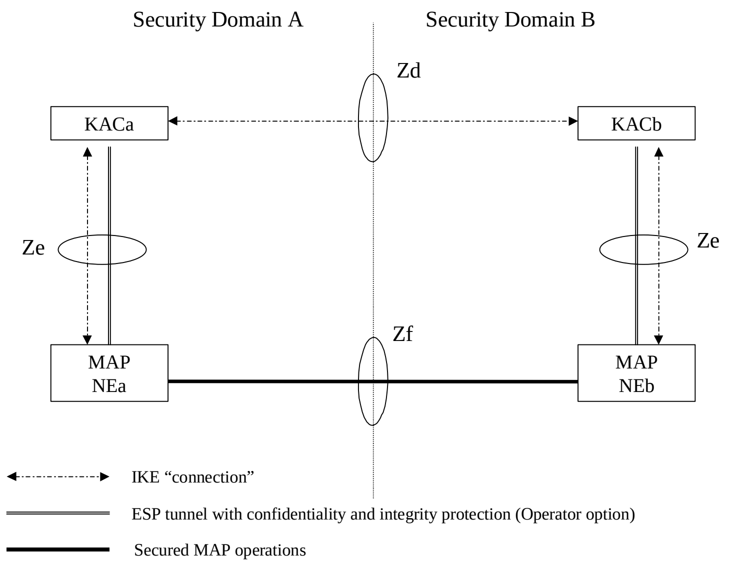

Figure 1. Security Architecture for MAP signalling traffic.

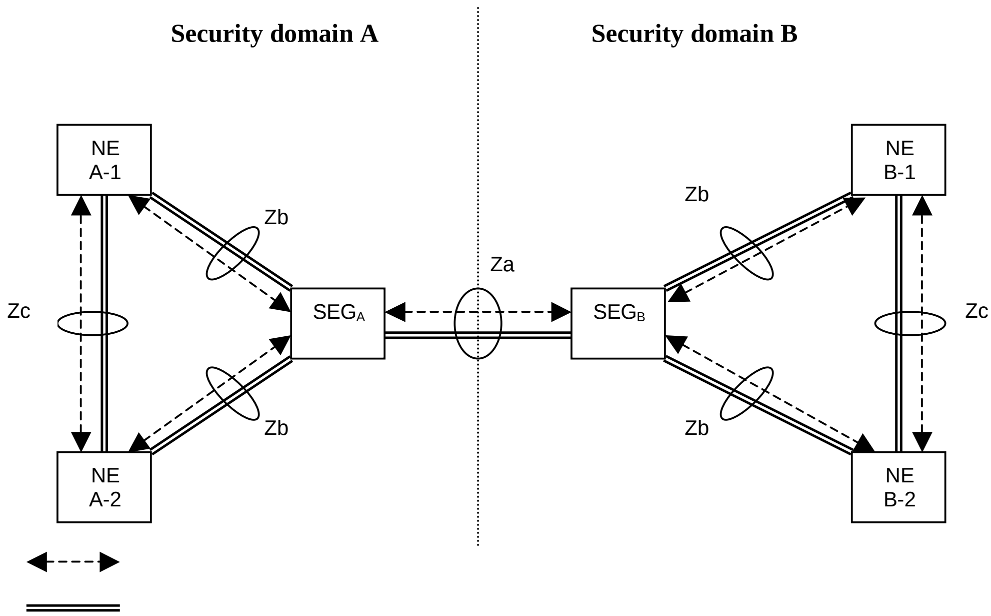

Figure 2. Security Architecture for IP signalling traffic.

The 3GPP SA3 document 33.200 defines in Appendix A a profile that limits the amount of features that needs to be supported in the UMTS network environment. The purpose of this profile is to limit the cost and complexity of equipment, as well as to promote interoperability. It does not, however, limit vendors in providing additional functionality or future versions of the standard to require additional mandatory behaviour. Currently, the following limitations have been set:

- No IP compression protocol
- No AH, only ESP
- NULL encryption not allowed
- Only tunnel mode is mandatory
- AES instead of DES

However, not much has yet been said regarding IKE and there are further details that we may want to say about IPsec. From a complexity reduction standpoint, it is more important to concentrate on IKE than on IPsec, as the former is more complex.

For the above reasons this document has been put together. This document does not take a stand on phasing issues e.g. in which standard release IKE should be supported in a particular interface. Instead, the intention of this document is to simply specify what kind of IKE should be supported, when that becomes necessary.

3 IKE Profile for MAP DOI

Ericsson's opinion of this has been described in the –01 version of the Internet-Draft. Here are the main points. The requirements set forth in the IKE and IPsec DOI MUST be followed with the exception of the following:

- Only Phase 1 of IKE is used, the rest is as defined by the MAP DOI.
- Only IPv6 is mandatory. Since the UMTS networks will be largely based on IPv6, we see no purpose mandating IPv4 IPsec.
- Perfect Forward Secrecy (PFS) SHOULD be supported in Phase 2. This will limit the CPU requirements set for a KAC node (with the cost of some additional security).
- In contrast to the requirements set in RFC 2409, Aggressive Mode MUST be implemented and Main Mode SHOULD be implemented. This will limit the complexity of the KAC and the delays in setting up SAs (with the cost of some additional security against DoS attacks).
- Only one identity type, ID_FQDN, MUST be implemented for phase 1. Other identity types specified in RFC 2407 SHOULD be implemented. This will limit the complexity needed for implementing and configuring KAC nodes.
- Only the 3DES encryption algorithm SHA1 algorithms MUST be implemented as ISAKMP encryption and hash operations. This is necessary since there is no AES-based hash-algorithm definition for IKE yet in the IETF.
- SA lifetime notifications will not be allowed, in order to limit complexity of protocol machinery and to ensure that SAs on both sides time out at exactly the same time.

- SA deletion will not be allowed (this is required in order to ensure that pull-based schemes can be used between network elements.
- Note that IKE specifies that all implementations MUST support authentication through pre-shared secrets and SHOULD support public key based authentication.

4 IPsec Profile

This section lists those additional profiling restrictions that Ericsson thinks should be adopted:

- Only IPv6 version of IPsec is mandatory.
- Only the HMAC_SHA1 algorithm is mandatory. This will limit the number of algorithms each node has to support.
- The support for bundles is optional [RFC 2401 section 4.3]. This will limit the complexity of the policy mechanisms in each node.
- Only the following components are mandatory for the Security Policy Database and selectors [RFC 2401 section 4.4]: source and destination addresses and ports, and transport protocol. Only single values, value-mask pairs, and wildcard values are mandatory for these. This will also limit the complexity of the policy mechanisms in each node.

5 IKE Profile

This section lists those profiling restrictions that Ericsson thinks should be adopted.

For IKE phase 1:

- Only the FQDN identity type is mandatory.
- Only aggressive mode is mandatory.
- Only preshared secrets are mandatory. This will make it possible to build KACs without integrated public key –based authentication support and PKI interfaces.
- Only the AES and SHA1 are mandatory for protection of IKE itself.

For IKE phase 2:

- PFS is optional [RFC 2409 section 3.3]
- Only IP addresses or subnets identity types are mandatory [RFC 2407 section 4.6.2.1]. Support for protocol and port numbers is mandatory.
- Notifications are mandatory [RFC 2408, 2407]

6 Open Questions

This section lists some issues regarding the profiles that we think are still open:

- Ericsson believes only IPv6 should be mandatory in all interfaces crossing operator boundaries. However, should IPv6 be mandated also on internal interfaces, such as the NE-KAC? Tentatively, we propose that the answer should be IPv6 allover.

- Are there interfaces such as the NE-KAC where SA3 could make ISAKMP/IKE optional and not mandatory? This relates to the phasing issues, and is not discussed further in this document. We just note that the possibility exists.
- Which integrity protection algorithm should be employed in IPsec and IKE? One of the current ones, or AES-MAC / SHA-256? Tentatively, we propose the answer should be the following: everything standardized in Release 4 should use SHA1 since only that is currently defined by IETF. In the next releases, we can likely use new IETF work, making then AES-MAC/SHA-256 a better option.

6 Conclusion and Discussion

Ericsson proposes these additional limitations to the profiles presented in Appendix A of 33.200, and that the open questions be discussed and resolved.

IPsec, IKE, MAPSEC DOI Profiles for the 3GPP

Contribution #91 and #101

Jari Arkko

Ericsson

Jari.Arkko@ericsson.com

Contents

- Reasons for profiling
- Current profile
- MAP DOI IKE profile
- IPsec Profile
- IKE Profile
- Open Issues

Reasons for Profiling

- Limit cost
- Limit complexity
- Improve interoperability through a common agreement of the minimum acceptable functionality

- Does not limit vendors in providing additional functionality
- Does not limit 3GPP in requiring additional functionality in the future

Current Profiles from 33.200

- No IP compression protocol
- No AH, only ESP
- NULL encryption not allowed
- Only tunnel mode is mandatory
- AES instead of DES

Can we say more regarding IPsec?

Should we say something about IKE?

Differences in the profiles wrt KAC-KAC, SEG-SEG, etc?

ERICSSON

MAP DOI IKE Profile

- Only Phase 1 of IKE is used, the rest is MAP DOI
- Only IPv6 is mandatory
- Perfect Forward Secrecy (PFS) optional: Limits CPU requirements
- Aggressive mode to be mandatory, main mode optional: Limits complexity,loses some security against DoS
- Only FQDN identities to be mandatory: Limits complexity

MAP DOI IKE Profile Cont’d

- AES, SHA1 used for protection of IKE: No AES-based hash yet in the IETF
- SA lifetime notifications will not be allowed: Limits complexity, ensures simultaneous timeout
- SA deletion will not be allowed: Allows pull-based mode to work
- Also note that IKE mandates preshared secrets, public-key based mechanisms are optional

Additional IPsec Profiling

- Only IPv6 is mandatory
- Only HMAC_SHA1 is mandatory
- Make support of bundles (nested SAs) optional
- Do not require all policy and selector mechanisms. Only addresses, ports, and transport protocol are mandatory. Only single values, address masks, and wildcards are the required values for these.

IKE Profiling

- Phase 1
  - Only IPv6 is mandatory
  - Aggressive mode to be mandatory, main mode optional: Limits complexity,loses some security against DoS
  - Only FQDN identities to be mandatory: Limits complexity
  - Also note that IKE mandates preshared secrets, public-key based mechanisms are optional: Enables building SEG/NE nodes without public key support and PKI interfaces
  - Only AES and SHA1 (or AES-MAC) are mandatory

IKE Profiling Cont’d

- Phase 2
  - Perfect Forward Secrecy (PFS) optional: Limits CPU requirements
  - Only IP address or subnet identity types are mandatory (IPv6)
  - Notifications are mandatory.

Open Issues

- It is clear to us that IPv6 should be used on all inter-operator interfaces. What about intra? Tentative answer: IPv6 in there as well.
- Are there interfaces on which 3GPP could make IPsec mandatory but IKE optional?
- Which integrity protection algorithm should be employed by IPsec and IKE? Tentative answer: SHA1 now for interfaces that are defined for Relese 4, later releases can use newer IETF work.