3GPP TSG SA WG3 Security – S3#23 **S3-020215**

14 - 17 May 2002

Victoria, BC, Canada

Source: **SSH Communications Security Corp**

Title: **IPSec Security Indicator**

Document for: **Discussion**

Agenda Item: **T.B.D**

1. Introduction

S3-010581 Proposed CR to 33.102: Configurability of cipher use (Rel-5) [1] was presented at S3#21 in Sophia Antipolis. The document considered only the indication of access network encryption. However, IMS is essentially an overlay to the PS-Domain and a separate security associations are required between the multimedia client and the IMS. Therefore the access network security indicator has not much meaning in multimedia connections.

This contribution discusses a security indicator of IMS connections.

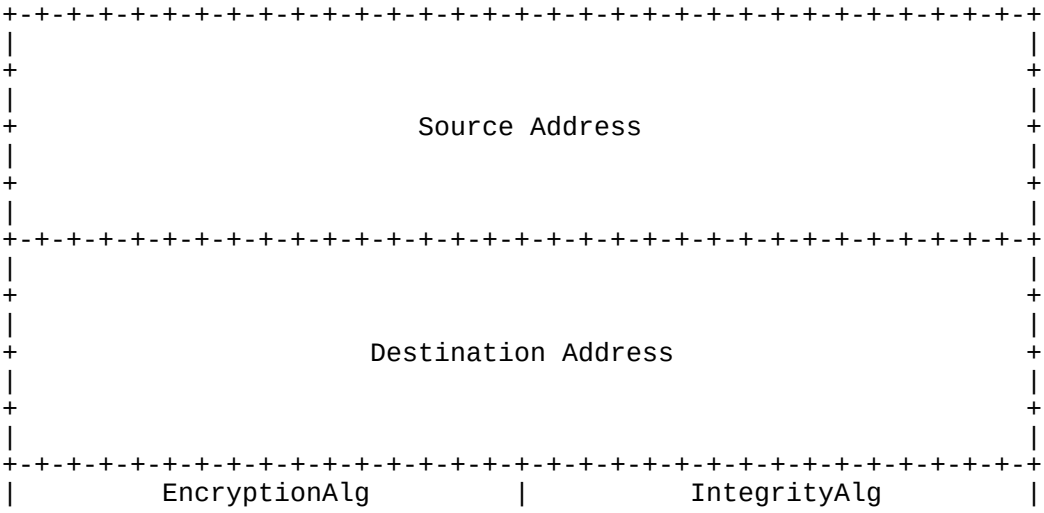
2. Indication of Security Association in IMS

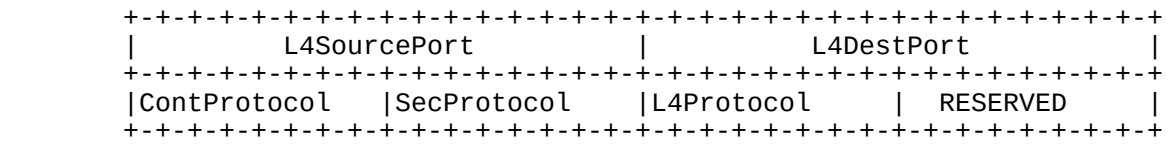
Since the protection between UE and P-CSCF is provided using IPSec ESP, the security association is visible only at the network layer. IPSec implementations have no standard mechanism in passing information about active SAs to application layer, but necessary information is required to indicate whether the security (data origin integrity and no confidentiality OR data origin authentication and confidentiality) is provided for the multimedia connection.

In IPSec implementations, there is usually a policy manager or relative functionality that takes care of IPSec policy and SA management and has the necessary information to indicate the security level to the application layer. To carry this information to application layer, policy manager should send a signal to upper layers describing the security parameters of active connections.

Security Indicator

The signal send from the IPSec policy manager should contain the following information:





Source Address	= 128-bit IP address of UE
Destination Address	= 128-bit IP address of P-CSCF
EncryptionAlg	= 16-bit Used encryption algorithm
IntegrityAlg	= 16-bit Used data origin authentication algorithm
L4SourcePort	= 16-bit layer 4 port number of UE
L4DestPort	= 16-bit layer 4 port number of P-CSCF
ContProto	= 8-bit container protocol (IPv6 or IPv4)
SecProtcol	= 8-bit security protocol (AH or ESP)
L4Protocol	= 8-bit layer 4 protocol (TCP, UDP or SCTP)
RESERVED	= 8-bit reserved for future use.

The order and length of the parameters are only illustrative (but mostly taken from sources such as RFC 2409: The Internet Key Exchange (IKE) [3]).

Every time a new SA is installed between UE and P-CSCF, policy manager should send the security indicator signal to the application layer. From this signal, application layer is capable of determining the provided level of security.

3. IETF Considerations

The interface between a policy manager and the application layer is not standardized at IETF (apart from very limited definition in RFC 2367 (PF_KEY Key Management API, Version 2 [2]). RFC 2367 is also only an informational RFC with no standards status – updating RFC 2367 might not confront much objections at IETF, but adding a security indicator signal to it would most probably be heavily objected by IETF.

As discussed at the mailing list, 3gpp_tsg_sa_wg3@list.etsi.fr, all the parameters needed to use IPSec/ESP for SIP do not need to be specified in IETF RFC, the security indicator for IMS connections could be included to the same document as above parameters.

4. Proposal

SA3 #23 are asked to discuss the necessity of the IPSec SA indicator signal for rel-6.

Reference

[1] 3GPP TD S3-010679, “Change request: Configurability of cipher use”, November 2001.
< ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_21_Sophia/Docs/PDF/S3-010679.pdf >

[2] D. McDonald & C. Metz & B. Phan, “RFC 2367: PF_KEY Key Management API, Version 2”, July 1998.

[3] D. Harkins & D. Carrel, ”RFC 2409: The Internet Key Exchange (IKE)”, November 1998.