Network Working Group
Internet-Draft
Expires: February 10, 2005

F. Dupont
GET/ENST Bretagne

August 12, 2004

IPsec transport mode in Mobike environments
draft-dupont-mobike-transport-00.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies how to use IPsec transport mode security associations in a Mobike environment, i.e., in an environment with sequential (mobility) or parallel (multi-homing) addresses.

1. Introduction

Mobike deals with "peer addresses" which are the addresses IKE runs over and which are the addresses used as outer addresses by tunnel mode IPsec security associations between security gateways [RFC2401bis]. Mobike both specifies in IKEv2 [IKEv2] a way to define alternate peer addresses and a way to update security associations, when one or both parties are mobile or multi-homed.

But transport mode IPsec security associations are end-to-end and have no outer addresses: they cannot be managed by Mobike, for instance, they cannot be updated. But there is an indirect way to take benefits from Mobike: assume that the peer addresses are the addresses of peers. This document uses the standard keywords [keywords] to indicate requirement levels.

2. Transport mode and addresses

The endpoint addresses of an IPsec transport mode security association are usually addresses of the peers but are taken from the traffic selectors, not from the peer addresses. When they are not the same than the peer addresses, they MUST be authorized by the local policy.

When a Mobike mechanism provides peer address lists or sets as described in section 3.1 of the Mobike design document [MOBIKE], this rule can be relaxed into: by default, any peer address MAY be used as an endpoint address of an IPsec transport mode security association.

3. Two examples

The first example is the IPv6 mobility [MIPv6] where a mobile node uses two addresses:

- the fixed home address in the remote/home network;
- transient care-of addresses assigned in the local/visited network.

In communications with its home agent, a mobile node uses a care-of address (because its home address is not usable until the home registration) so its peer address is a care-of address. But to protect the mobility signaling [MN-HA] a transport mode IPsec security association pair is established using the home address.

Using a Mobike peer address management (as in [ADDRMGT]) a mobile node can add its home address as an alternate peer address and be authorized to use it in its traffic selector for the mandatory transport mode IPsec security association pair. Note the other IPsec security associations, in tunnel mode, are updated in case of handoffs by the mobility support itself, not by Mobike.

The second example is multi-homing using SCTP [SCTP], itself or what we call the SCTP model of multi-homing, between two hosts. A multi-homed peer can register using a Mobike mechanism its addresses as peer addresses and is authorized to use them to build transport mode IPsec security associations using only one IKE session, aka IKE security association. Note this document does not address the question of using multiple simultaneous addresses in IPsec security associations in the outgoing side, even if the main implementation issue, the address selection, does not exist for transport mode.

4. Acknowledgments

The MOBIKE Working Group agreed at the 60th IETF meeting in San Diego to put transport mode ouside of its immediate scope. But as transport mode can take indirect benefits of Mobike mechanisms, an as short as possible document (this one) was proposed.

Some special transport mode IPsec security associations over IP-IP tunnels [VPN] were proposed for consideration by Joe Touch but in fact they are another example of security associations which are updated by an external (to IPsec) mechanism, i.e., as in the IPv6 mobility case, Mobike mechanisms can only help to easily solve authorization issues.

5. Security Considerations

IKEv2 and Mobike mechanisms do verify that the primary peer address (for IKEv2) and further alternate peer address (for Mobike mechanisms) are correctly authenticated and authorized, so they MAY safely be used for transport mode IPsec security associations as endpoint addresses.

6. References

6.1 Normative References

[keywords] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.

6.2 Informative References

[ADDRMGT] Dupont, F., "Address Management for IKE version 2", draft-dupont-ikev2-addrmgmt-05.txt (work in progress), June 2004.

[IKEv2] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-14.txt (work in progress), May 2004.

[MIPv6] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[MN-HA] Arkko, J., Devarapalli, V. and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[MOBIKE] Kivinen, T., "Design of the MOBIKE protocol",

draft-ietf-mobike-design-00.txt (work in progress), June 2004.

[RFC2401bis] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", draft-ietf-ipsec-rfc2401bis-02.txt (work in progress), April 2004.

[SCTP] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[VPN] Touch, J., Eggert, L. and Y. Wang, "Use of IPsec Transport Mode for Dynamic Routing", draft-touch-ipsec-vpn-07.txt (work in progress), February 2004.

Author's Address

Francis Dupont
GET/ENST Bretagne
2 rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

Fax: +33 2 99 12 70 30
EMail: Francis.Dupont@enst-bretagne.fr

Intellectual Property Statement

Full Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.