Internet Engineering Task Force
INTERNET DRAFT
Expires in August 2004

Francis Dupont
GET/ENST Bretagne

February 2003

Address Management for IKE version 2

<draft-dupont-ikev2-addrmgmt-04.txt>

Status of this Memo

Abstract

The current IKEv2 proposal [1] lacks an address management feature. As it is compatible with the NAT traversal capability, this document specifies a complete address management with support for multi-homing and mobility, and fulfill mobike working group [2] goals 1, 2, 3, 4, and 6 (for goal 5 look at [3]).

1. Introduction

In this document, the addresses used to transport IKE messages are named the "peer addresses" (term introduced by [4]). These peer addresses should no more be directly or indirectly included in identities ([5] and [6]) as it is commonly done for IKEv1.

The current IKEv2 draft [1] often makes the assumption that an address identifies a node when nodes behind a NAT can share the same address and a node can use many different addresses. This must be taken into account in implementations, for instance by reading this document before writing code...

This document describes the goals of an address management for IKEv2, including the requirements for multi-homing and mobility support, and finishes by a concrete proposal.

In this document, open questions are introduced by the word NOTE.

2. Goals

The goals of the address management proposed in the document can be divided in some general goals and in requirements for the three mechanisms which can change the peer addresses.

2.1 Simplicity, Performance and Security

The address management should be as simple as possible, i.e., it should introduce minimal additions to the current IKEv2 draft [1] and each addition should be justified.

The performance is an important criterion. For instance, rekeying can update the peer addresses of an IKE SA or an IPsec SA pair, but rekeying is too expensive and a specific solution is needed.

As a security protocol, IKEv2 should get a high security level. Unfortunately we already showed that the NAT traversal feature comes with a security issue (the transient pseudo-NAT attack [7]). Such problems introduced by the peer address flexibility must be described in this document and at least be mitigated by options in configurations. For instance, the NAT traversal feature should never be enabled when one knows that there can not be a NAT as today in IPv6.

An other example of an insecure mechanism is to use the addresses in IP headers of CREATE_CHILD_SA messages as the endpoint addresses of the new IPsec SAs without further control on them: peer addresses must be managed.

2.2 Terminology

The addresses of the two peers are named "peer addresses". The primary peer address of a peer is initialized to the address used to transport messages of the initial exchanges, other addresses are "alternate peer addresses".

The proxy case is the setup of transport mode IPsec SAs on the behalf of another party, i.e., transport mode IPsec SAs where the traffic selectors do not match the primary peer addresses.

2.3 Multi-homing requirements

In this document, the support of multi-homing is the support of nodes with several global addresses. Some of the addresses can be "better" than others, or "better" for some destinations. Some can, from time to time, be unavailable.

The main requirement for the support of multi-homing is the management of a set of peer addresses for each peer. The set can be partially ordered or some subset can be loosely associated with some destinations (i.e., some subset of the other peer address set).

For the communication between multi-addressed hosts, the support of the proxy case can be useful because it provides an easy way to setup transport mode IPsec SAs with different addresses from one IKE SA. In such cases the other party is in fact the same host, this dramatically simplifies the authorization issue.

2.4 Mobility requirements

In the context of Mobile IPv6 ([8] and for the special case of Home Agents [9]), the interaction of Mobility and IPsec was analyzed in another document [10]. This document assumes an IPv6 context as Mobile IPv6 is the most powerful mobility proposal available today.

An IPv6 mobile node is another type of multi-addressed node with:
- a care-of address in a prefix of the visited link.
  The care-of address is used to route packets.
- the home address in a prefix of the home link.
  The home address is used to identify the mobile node.

The care-of address is transient and usually the mobile node can not provide a proof that it is the node using it. So it must be trusted and a return routability check (i.e., an enforced answer from this address) should be used if it is not.

With a common correspondent, the mobility is transparent and there is no reason to use another address than the home address. For optimized schemes, without an implementation of header compression in ESP tunnel mode (mobile's goal 5 [2]) the choice between a transport mode using triangular routing (IPsec can be used to verify home address options) and a tunnel mode with routing optimization is not clear. But this case does not add

new requirement, i.e., the home agent case includes them.

With the home agent, there are three main cases (c.f. [9]):

- The mobility signaling which is mandatory protected and raises a specific issue in its initial phase: the IKE SA must be setup using the care-of address as the peer address but this IKE SA is used to build an IPsec SA pair with the home address as traffic selector. This IPsec SA will protect the home registration which will make the home address available. This can be considered as a specialized proxy case.

- Other genuine communications between the home agent and the mobile node can be covered by the proxy case support too. Note this is the only case at the exception of signaling where mobility behaves in a different way than a mobile IPsec VPN (so we proposed to relax the corresponding rule in a future version of [8] and [9]).

- The traffic relayed by the home agent through a tunnel with the mobile node can be partially or fully protected by IPsec SA pair(s). Encapsulation should be performed only once, including for degenerated (but not for free) encapsulation like the home address option or the mobility routing header.

In all cases of interaction with the home agent, the mobile node peer address should be a care-of address. When the mobile node moves, another care-of address is used and some SAs, including the IKE SA, must be updated to use the new address.

Usually the previous peer address is no more usable. In order to avoid a trivial denial of services, a strong sequencing of updates is required with a way to cancel possible pending updates when fast multiple handoff happen.

The IPsec pair which protects the mobility signaling uses the home address as its traffic selector for the mobile node. It must not be updated at each handoff. The update mechanism must provide a fine grain (i.e., per SA) update.

3. Proposal

The proposal for an address management in IKEv2 is spawn from the NAT traversal mechanisms, mainly with a new peer address update payload. But there are some points that have to be kept as they are in the current IKEv2 draft [1].

3.1 Kept points from draft 06

The peer addresses are used to transport messages. The reply to a request MUST be sent to the source of the request from the destination request, i.e., addresses and ports are reversed between the request and its reply. There is no exception to this rule.

For tunnel mode IPsec SAs, the endpoint addresses are the primary peer addresses. We don't propose an alternate way to specify them. The same requirement applies to transport mode IPsec SAs at the exception of the proxy case.

3.2 Small points

In retransmission of requests or responses, copies of messages do not include peer addresses. So a peer MAY retransmit an IKE message from or to a different address.

The primary peer addresses are IKE SA parameters and are specified by the IKE_SA_INIT exchange. Note that when NAT traversal is not active, they are implicitly protected by the NAT_DETECTION notifications.

All the text below applies only to the case where NAT traversal is not active.

In the proxy case, the initiator is acting as a client negotiator on the behalf of another party. The address of this other party is sent in the initiator traffic selector and will become the address of this end of the transport mode IPsec SA pair. A proper authorization in the local policy of the responder is REQUIRED, the defaults SHOULD be:

- using an alternate peer address set is permitted
- other cases are denied.

3.3 Peer address notifications

The peer address notifications are copied from the current NAT-DETECTION-SOURCE-IP and NAT-DETECTION-DESTINATION-IP notifications. They includes the peer source or destination address with its family and an operation code. They MUST be in an encrypted payload. Operations are PRIMARY, ADD and DELETE (last two for alternate addresses).

All messages after the first exchange involving an alternate peer address MUST include at least one peer address notification for each peer, i.e., at least one for the source and at least one for the destination.

Such messages belong to IKE_AUTH or CREATE_CHILD_SA exchanges, or carry the peer address update payload defined below.

They provide a cryptographically proof of no alteration en-route of the peer addresses and operations on the sets of peer addresses, i.e., change of the primary peer address of a peer, addition to and deletion from the peer address set of a peer.

When the peer address notifications are not supported, the capability to use an alternate peer address, and only this, is lost.

3.4 Explicit peer address update payload

A new payload has to be defined for an explicit peer address update mechanism. We propose to copy it from the delete payload, see Annex B.

The new peer address update payload has strong sequencing requirements. IKEv2 messages have a protected sequence number so the only sequencing issues are the window of processing and pending exchanges. Any messages with a peer address update payload MUST be processed in order.

When the receiver of an update request has to check the validity of the new primary peer address, it MAY use a return routability check sending an informational request at the new address and waiting for an answer. As informational exchanges are protected no more is needed.

Example of a return routability check:

```
  I --- address update request --> R
  I <-- informational RR request - R
  I --- informational RR reply --> R
   now the responder knows the initiator should be where it
   claimed to be.
  I <--- address update reply ---- R
```

As for the delete payload, the peer address update payload specifies the SPIs of the IPsec and IKE SAs it applies to. But a simple way to specify all SAs (i.e., the IKE SA and all the tunnel mode IPsec SAs it negotiated) is needed so is provided.

4. Security Considerations

Great care was used to avoid to introduce security threats.

The NAT traversal feature comes with a security flaw (the transient pseudo-NAT attack [7]) which can not be easily avoid. IMHO the NAT traversal feature should be enabled only when the presence of NATs is likely/possible.

When the NAT traversal feature is disabled, the address of the other peer can not be changed en-route by an attacker but the proofs the peer is really at its address are:
- the trust in the peer
- the proof that the peer can receive messages sent to its address

The second (a.k.a. the return routability check) works only with at least three messages, i.e., for the initial exchange (with the address stability requirement) and for the explicit optional checks. IMHO these checks SHOULD be required by default.

5. Acknowledgments

The rare people in the Mobility world with IPsec interests, or in the IPsec world with Mobility interest, should receive all thanks because without them we (me and all the future co-authors) have given up for a long time.

Tero Kivinen helped to improve the NAT traversal part of this proposal. Tero and Jari Arkko proposed another form of peer address update based on the IKE SA addresses.

7. Normative References

None?

8. Informative References

[1] C. Kaufman, ed., "Proposal for the IKEv2 Protocol", draft-ietf-ipsec-ikev2-12.txt, January 2004.

[2] IKEv2 Mobility and Multihoming (mobike), "charter", http://www.ietf.org/html.charters/mobike-charter.html.

[3] J. Vilhuber, "IP header compression in IPsec ESP", draft-vilhuber-hcoesp-00.txt, January 2003.

[4] B. Korver, E. Rescorla, "The Internet IP Security PKI Profile of ISAKMP and PKIX", draft-ietf-ipsec-pki-profile-03.txt, July 2003.

[5] P. Hoffman, "Adding revised identities to IKEv2", http://www.vpnc.org/ietf-ipsec/, Message-Id: <p05200f06b9edf48ac57b@[165.227.249.18]>, November 2002.

[6] M. Kaat, "Overview of 1999 IAB Network Layer Workshop", RFC 2956, October 2000.

[7] F. Dupont, J.-J. Bernard, "Transient pseudo-NAT attacks or how NATs are even more evil than you believed", draft-dupont-transient-pseudonat-03.txt, February 2004.

[8] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24.txt, June 2003.

[9] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents", draft-ietf-mobileip-mipv6-ha-ipsec-06.txt, June 2003.

[10] F. Dupont, W. Haddad, "How to make IPsec more mobile IPv6 friendly", draft-dupont-ipsec-mipv6-05.txt, February 2004.

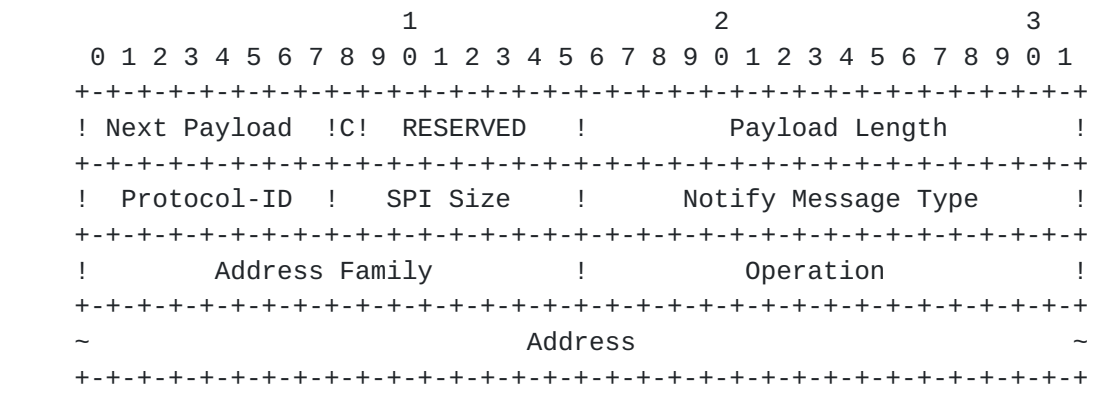
[11] D. McDonald, C. Metz, B. Phan, "PF_KEY Key Management API, Version 2", RFC 2367, July 1998.

9. Author's Address

Francis Dupont
ENST Bretagne
Campus de Rennes
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

Annex A. Peer Address Notification Format.

The following diagram illustrates the content of the Peer Address Notification:



The notification header is for IKE SA (Protocol-ID 0, SPI Size 0 and no SPI. The Address Family is from IANA Address Family Numbers (IPv4 is 1 and IPv6 2). The proposed names are PEER-ADDRESS-SOURCE and PEER-ADDRESS-DESTINATION, with 248XX. Operation codes are:

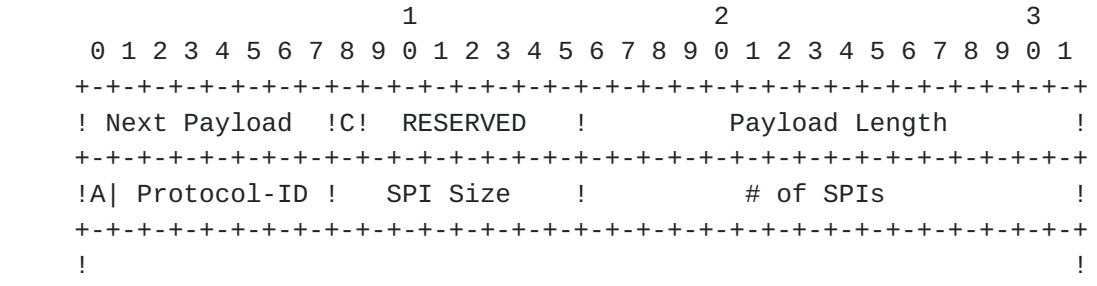
- PRIMARY (1): the address is the primary peer address. The peer address update payload MUST be used to change it.
- ADD (2): add a new alternate peer address to the set.
- DELETE (3): delete an alternate peer address from the set.

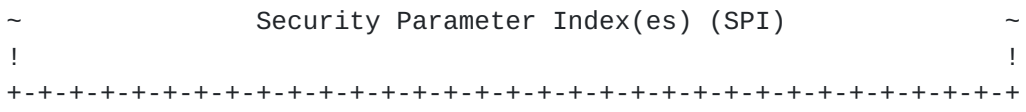
Annex B. Peer Address Update Payload Format.

The next figure 17 shows the format of the Peer Address Update Payload. It is possible to send multiple SPIs in a Peer Address Update payload, however, each SPI MUST be for the same protocol. Mixing of Protocol Identifiers MUST NOT be performed in a the Peer Address Update payload. It is permitted, however, to include multiple Peer Address Update payloads in a single INFORMATIONAL Exchange where each Peer Address Update payload lists SPIs for a different protocol.

Update of the IKE_SA is indicated by a Protocol_Id of 0 (IKE) but no SPIs. Update of a CHILD_SA, such as ESP or AH, will contain the Protocol_Id of that protocol (1 for ESP, 2 for AH) and the SPI is the SPI the sending endpoint would expect in inbound ESP or AH packets.

The following diagram illustrates the content of the Peer Address Update Notification:




~ Security Parameter Index(es) (SPI) ~
!

- All (1 bit) - MUST be set to one when all SAs (the IKE SA and all tunnel mode outgoing IPsec SAs negotiated by it) are updated. In this case the update is for the IKE-SA (Protocol-ID 0, SPI size 0, no SPI and number of SPIs 0). MUST be set to zero when an individual SA is updated.

- Protocol_Id (7 bits) - Must be zero for an IKE_SA, 1 for ESP, or 2 for AH.

- SPI Size (1 octet) - Length in octets of the SPI as defined by the Protocol-Id. Zero for IKE (SPI is in message header) or four for AH and ESP.

- # of SPIs (2 octets) - The number of SPIs contained in the Peer Address Update Notification. The size of each SPI is defined by the SPI Size field.

- Security Parameter Index(es) (variable length) - Identifies the specific security association(s) to delete. The lengths of these fields are determined by the SPI Size and # of SPIs fields.

ESP and AH SAs always exist in pairs, with one SA in each direction. When an SA is updated for a peer address, both members of the pair MUST be updated. When SAs are nested, as when data (and IP headers if in tunnel mode) are encapsulated first with IPcomp, then with ESP, and finally with AH between the same pair of endpoints, all of the SAs MUST be updated together. Each endpoint MUST update the SAs it receives on and allow the other endpoint to update the other SA in each pair.

To update a peer address of an SA, an Informational Exchange with one or more peer address update payloads is sent listing the SPIs (as they would be placed in the headers of inbound packets) of the SAs to be updated, and with a peer address notification setting the primary peer address. The recipient MUST update the designated SAs. Normally, the reply in the Informational Exchange will contain peer address update payloads for the paired SAs going in the other direction. Note there is no special case for update collision.

The proposed name is the Update (U) payload.

Annex C. PF_KEY version 2 SADB_X_ADDUPD

This annex describes an extension to PF_KEYv2 [11] which provides a way to ask a peer address update of an IPsec SA and all its siblings (i.e., an update with the All flag set to one).

The format of the message is:
<base, SA(*), address(SD), new_address(SD)>
and is sent the registered socket listeners by or via the kernel.
No answer is needed because if it fails it will be done again.

New values are needed for SADB_X_ADDUPD and for
SADB_X_EXT_NEW_ADDRESS_SRC and SADB_X_EXT_NEW_ADDRESS_DST
which should have the same layout than SADB_EXT_ADDRESS_*,
i.e., sadb_address structure.

NOTE: IKE itself needs a PF_KEYv2 extension for individual
updating of an IPsec SA.