Network Working Group	S. Sugimoto
Internet-Draft	Ericsson
Intended status: Informational	F. Dupont
Expires: June 17, 2008	CELAR
	M. Nakamura
	Hitachi
	December 15, 2007

TOC

PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE draft-sugimoto-mip6-pfkey-migrate-04

Status of this Memo

Abstract

This document describes the need for an interface between Mobile IPv6 and IPsec/IKE and show how the two protocols can interwork. We propose a set of extensions to the PF_KEY framework which allows smooth and solid operation of IKE in a Mobile IPv6 environment. The first extension is called PF_KEY MIGRATE and is for migrating the endpoint addresses of a IPsec Security Association pair in tunnel mode. The second extension is named SADB_X_EXT_PACKET and allows IKE to make the right choice for address selection in bootstrapping process. Both extensions are helpful for assuring smooth interworking between Mobile IPv6 and IPsec/IKE and achieving performance optimization.

Table of Contents

1. Introduction

TOC

In Mobile IPv6 (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.) [RFC3775], the Mobile Node (MN) and the Home Agent (HA) use some IPsec Security Associations (SAs) in tunnel mode to protect some mobility signaling messages, mobile prefix discovery and optionally payload traffic. Since the MN may change its attachment point to the Internet, it is necessary to update its tunnel endpoint address of the IPsec SAs. This indicates that corresponding entry in IPsec databases (Security Policy (SPD) and SA (SAD) databases) should be updated when MN performs movements. In addition, IKE requires treatment to keep its IKE session alive in a Mobile IPv6 environment. This document describes the need for an interface between Mobile IPv6 and IPsec/IKE and shows how the two protocols can interwork. We propose

a set of extensions to the PF_KEY framework (McDonald, D., Metz, C., and B. Phan, "PF_KEY Key Management API, Version 2," July 1998.) [RFC2367] which allows smooth and solid operation of IKE in an Mobile IPv6 environment. The first extension is called PF_KEY MIGRATE and is for migrating the endpoint addresses of the IPsec SAs in tunnel mode. The second extension is named SADB_X_EXT_PACKET and allows IKE to make the right choice in address selection in the bootstrapping process. Both extensions are helpful for assuring smooth interworking between Mobile IPv6 and IPsec/IKE and achieving performance optimization.
In this document, the term IKE implicitly stands for both IKEv1 [RFC2409] (Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)," November 1998.) and IKEv2 [RFC4306] (Kaufman, C., "Internet Key Exchange (IKEv2) Protocol," December 2005.). In description with regard to any functionality that is specific to either of the protocols, specific protocol name shall be provided.

---

2. Needs for Interactions between Mobile IPv6 and IPsec/IKE

TOC

The section 4.4 of RFC 3776 (Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," June 2004.) [RFC3776] specifies the rules which applies to IKE for MNs and HAs. The first requirement is to run IKE over the Care-of Address (CoA) because the Home Address (HoA) is usable only after the home registration so not yet in the bootstrapping phase.
A tunnel IPsec SA pair protects some signaling messages and optionally all the traffic between the MN and HA. The initial SPD entry uses the HoA for the MN endpoint address and updates this address to the new CoA at each movement. A tunnel SA pair is created on demand and is updated too. The RFC 3775 (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.) [RFC3775] assumes there is an API which performs the update in the SPD and SAD on both the MN and HA. This document is mainly about this API.
Mobile IPv6 specifies a flag named Key Management Mobility Capability bit (K-bit) in Binding Update (BU) and Binding Acknowledgement (BA) messages (section 10.3.1 of [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.)), which indicates the ability of IKE sessions to survive movement. When both the MN and HA agree to use this functionality, the IKE daemons dynamically update the IKE session when the MN moves. In order to realize this, IKE daemons should be notified by Mobile IPv6, and necessary information to migrate the IKE session should be provided.
Mobile IPv6 may need to make an access to the SPD not only for updating an endpoint address but also for the deletion/insertion of a specific SPD entry. When the MN performs Foreign-to-Home movement, IPsec SAs established between the MN and HA should be deleted, which means that the SPD entry should have no effect any more. On the other hand, when

the MN performs Home-to-Foreign movement, the IPsec SAs should be restored. Hence security policy entries that are associated with tunnel mode SAs may dynamically be added/removed (enabled/disabled) in along with MN's movements.
It should be noted that NEMO Basic Support (Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," January 2005.) [RFC3963] has similar requirements for the Mobile Router (MR) and MR's HA (MRHA). In NEMO, the MR works just as same as a MN registering its location information to the MRHA and establishes a tunnel (IP-in-IP or IPsec tunnel). When an IPsec tunnel is established between MR and MRHA, the MR serves as a Security Gateway for the nodes connected to the mobile network. The MR is responsible for handling its tunnel endpoint properly.

---

3. Requirements

TOC

Given the need for an interface between Mobile IPv6 and IPsec/IKE, there should be a minimum interface between the two protocols. Followings are the requirements for the interface from a software engineering point of view.

- Necessary modifications to the existing software, namely Mobile IPv6 and IPsec/IKE, in order to realize proposed mechanisms, should be kept minimum.

- Proposed mechanism should not be platform dependent. The mechanism should be based on technology which is commonly available on various platform. This seems to be essential for achieving high portability of the implementation which supports proposed mechanisms.

---

4. PF_KEY Extensions for Mobile IPv6

TOC

In order to fulfill the needs and requirements described in Section 2 (Needs for Interactions between Mobile IPv6 and IPsec/IKE) and Section 3 (Requirements) we propose to extend the PF_KEY framework so that Mobile IPv6 and IPsec/IKE could interact with each other.

TOC

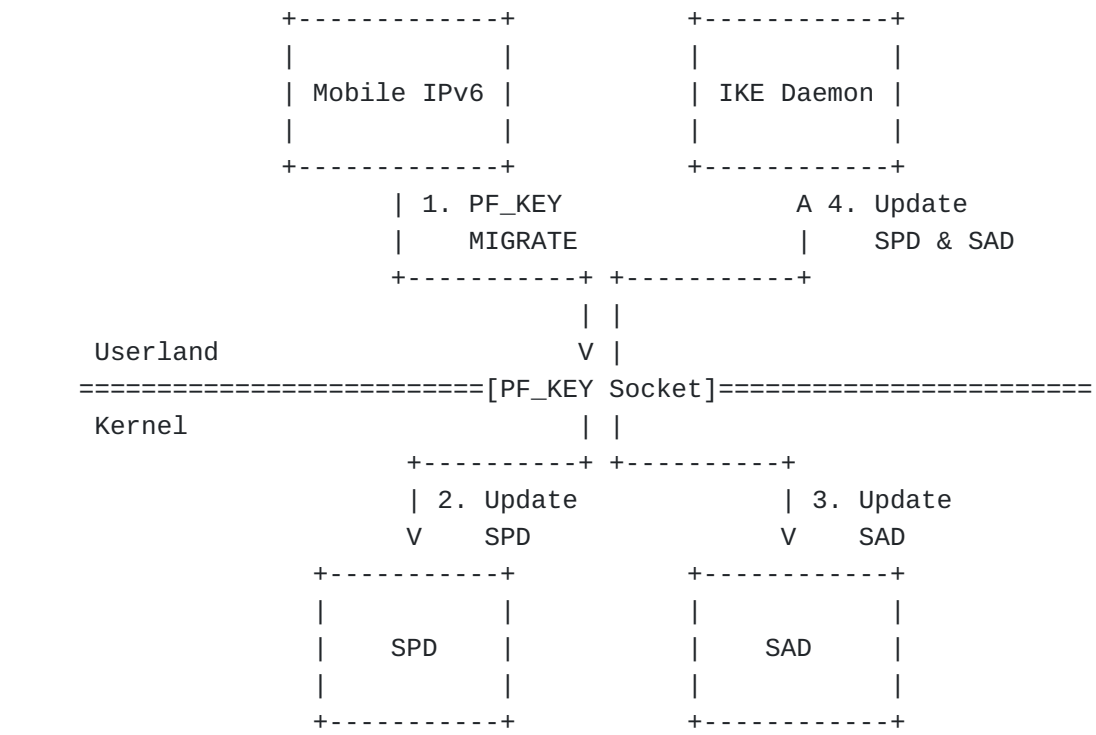
4.1. PF_KEY MIGRATE Message

The first extension is primarily for migrating an endpoint address of an IPsec SA pair in tunnel mode from one to another, which results in updating IPsec databases. A new PF_KEY message named MIGRATE is introduced for the mechanism.

4.1.1. Overview

TOC

The figure below illustrates how Mobile IPv6 and IPsec/IKE components interact with each other using PF_KEY MIGRATE messages in a dynamic keying scenario. On left top, there is a Mobile IPv6 entity. It may be possible that Mobile IPv6 component is completely implemented inside the kernel (this is the case for our implementations because it makes some facilities and extensions far easier at the cost of maintaining a SPD image in daemons). In any case, Mobile IPv6 should be the one which issues the MIGRATE messages. On right top, there is an IKE daemon which is responsible for establishing SAs required for Mobile IPv6 operation. In a manual keying scenario, the difference is only that there is no IKE daemon running on the system.



The primary role of PF_KEY MIGRATE messages is to migrate endpoint addresses of tunnel mode SA pairs requesting IPsec to update its databases (SPD and SAD). In addition, the new message can be used by IKE to enhance its mobility capability. When a PF_KEY MIGRATE message is properly processed by the kernel, it is sent to all open sockets as

normal PF_KEY messages. The processing of a sequence of MIGRATE messages is done in following steps:

*Mobile IPv6 issues a PF_KEY MIGRATE message to the PF_KEY socket.

*The operating system (kernel) validates the message and checks if corresponding security policy entry exists in SPD.

*When the message is confirmed to be valid, the target SPD entry is updated according to the MIGRATE message. If there is any target SA found that are also target of the update, those should also be updated.

*After the MIGRATE message is successfully processed inside the kernel, it will be sent to all open PF_KEY sockets.

*The IKE daemon receives the MIGRATE message from its PF_KEY socket and updates its SPD and SAD images. The IKE daemon may also update its state to keep the IKE session alive.

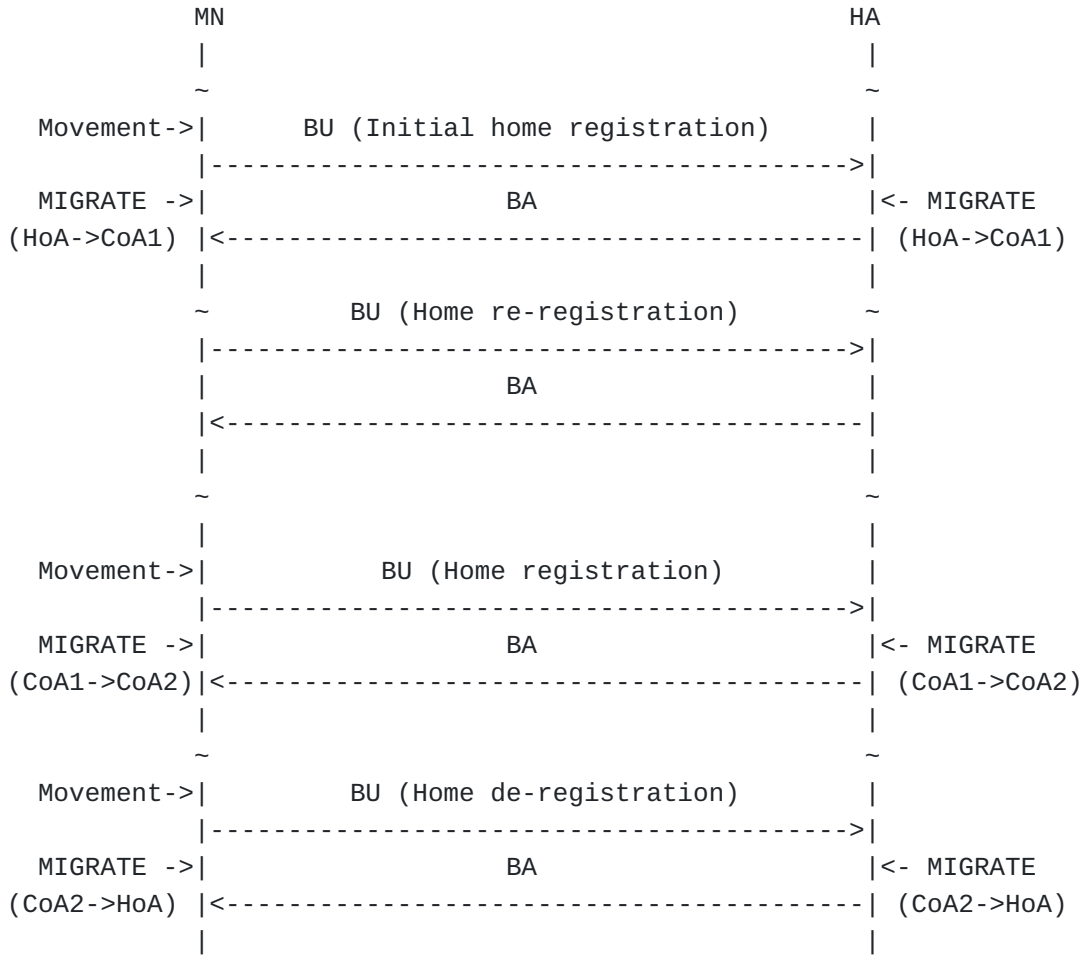
Note that the way IKE maintains its local copy of SPD (the SPD image) is an implementation specific issue since there is no standard interface to access SPD. Some IKE implementation may continuously monitor the SPD inside the kernel. Some IKE implementation may expect notification from the kernel when the SPD is modified. In either way, the proposed mechanism gives a chance for IKE to keep its SPD image up-to-date which is significant in Mobile IPv6 operation.

4.1.2. Message Sequence

TOC

Next, we will see how migration takes place in along with home registration. The figure below shows sequence of mobility signaling and PF_KEY MIGRATE messages while the MN roams around links. It is assumed that in the initial state the tunnel endpoint address for a given MN is set as its home address. In the initial home registration, the MN and HA migrate the tunnel endpoint address from the HoA to CoA1. It should be noted that no migration takes place when the MN performs re-registration since the care-of address remains the same. Accordingly, the MN performs movement and changes its primary care-of address from CoA1 to CoA2. A PF_KEY MIGRATE message is issued on both MN and HA for each direction. When the MN returns to home, migration takes place updating the endpoint address with the MN's home address.
With regard to the timing of issuing a MIGRATE message on the MN side, the message can be issued immediately after the home registration. That is, there is no need to wait until the acknowledgment from the HA to issue migrate the endpoint addresses stored in the IPsec databases. The

Mobile IPv6 specification ([RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.) Section 11.6.3) actually allows the MN to start using the new care-of address immediately after sending a BU message to the HA. This may help the MN to minimize the packet loss of its outbound traffic during the handover.



4.1.3. Issuing PF_KEY MIGRATE Message

TOC

The Mobile IPv6 entity (MN or HA code) triggers the migration by sending a PF_KEY MIGRATE message to its PF_KEY socket. Conceptually, the PF_KEY MIGRATE message should contain following information:

- *Selector information:
  - -source address/port
  - -destination address/port

-upper layer protocol (i.e., Mobility Header)

-direction (inbound/outbound)

*Old SA information:

-old source endpoint address

-old destination endpoint address

-IPsec protocol (ESP/AH)

-mode (Tunnel)

*New SA information:

-new source endpoint address

-new destination endpoint address

-IPsec protocol (ESP/AH)

-mode (Tunnel)

Selector information is required for specifying the target SPD entry to be updated. Basically the information should contain necessary elements which characterize traffic selector as specified in the IPsec architecture ([RFC2401] (Kent, S. and R. Atkinson, “Security Architecture for the Internet Protocol,” November 1998.), [RFC4301] (Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” December 2005.)). With regard to the upper layer protocol, when the Mobile IPv6 stack is not fully aware of IPsec configuration, an wild-card value could be given. In such case, an upper layer protocol information should not be taken into account for searching SPD entry. Plus, the direction of the security policy (inbound/outbound) should be provided. The old SA information is used to specify target security association to be updated. The source and destination addresses of the target entry should be overwritten with the ones included in the new SA information. Note that the IPsec protocol and mode fields should not be updated by a PF_KEY MIGRATE message.
A PF_KEY MIGRATE message should be formed based on security policy configuration and binding record. The selector information and some parts of the SA information (IPsec protocol and mode) should be taken from the policy configuration. The rest of the information should be taken from the sequential binding information. For example, in the case where the MN updates its inbound security policy and corresponding tunnel mode SA pair, the old source address should be set as its previous CoA, and the new source address should be set as its current

CoA. Hence, the MN should sequentially keep track of its CoA record. Such information shall be stored in binding update list entry. For the same reason, the HA should keep track of previous CoAs of MNs. Such information shall be stored in binding cache entry.
Additionally, a piece of information which indicates a mobility capability of IKE (K-bit) should be provided by any means. This makes it possible for IKE to see if there is a need to update its state (IKE endpoint addresses) in accordance with PF_KEY MIGRATE messages.
A detailed message format of PF_KEY MIGRATE is provided in Appendix A (PF_KEY MIGRATE Message Format).

4.1.4. Processing PF_KEY MIGRATE Message

TOC

Since a PF_KEY MIGRATE message is applied to a single SPD entry, the kernel should first check validity of the message. If the message is invalid, an EINVAL error MUST be returned as a return value for the write() operation made to the PF_KEY socket. After the validation, the kernel checks if the target SPD entry really exists. If no entry is found, an ENOENT error MUST be returned. If a SPD entry is found and successfully updated, a success (0) MUST be returned regardless of subsequent result of SAD lookup/update. Note that there may be a case where a corresponding SAD entry does not exist even if a SPD entry is successfully updated. In any error case, a PF_KEY MIGRATE message MUST NOT have any effect on the SPD and SAD.
With respect to the behavior of a normal process (including the IKE daemon) which receives a PF_KEY MIGRATE message from a PF_KEY socket, it SHOULD first check if the message does not include erroneous information. When there is any error indicated, the process MUST silently discard the PF_KEY MIGRATE message. Otherwise, the processing of the message may continue.

4.1.5. Applicability of PF_KEY MIGRATE to Other Systems

TOC

The PF_KEY MIGRATE extension can also be applied to other systems than Mobile IPv6. In some systems, there is a need to update endpoint address of IPsec security association for various reasons such as mobility management and multihoming.
In a Mobile VPN scenario (aka "road warrior"), client node roams around different IP subnets while maintaining security association with the security gateway. Just like the case in Mobile IPv6, both of the IKE peers need to update the endpoint of the IPsec tunnel and PF_KEY MIGRATE message can be used for the update.
In HIP mobility management scenario[I-D.ietf-hip-mm] (Henderson, T., “End-Host Mobility and Multihoming with the Host Identity Protocol,”

March 2007.), a mobile host can maintain a HIP association with its peer while moving around IP subnets. When the mobile host changes its attachment point to the Internet, it sends an UPDATE message to the peer reporting its new locator. Since HIP association is represented by an IPsec security association of ESP BEET mode, the same mechanism can be applied for the purpose of updating endpoint. The procedure of MIGRATE can take place when the mobile host detects movement and when the peer receives the UPDATE message.
From the ID/Locator separation point of view, PF_KEY MIGRATE is designed to update locators stored in an IPsec security association. Hence, the message can be applied to IPsec security association in tunnel mode. However, there are exceptional cases where IPsec security associations are bundled. In some case, a transport mode security association may be bundled with a tunnel mode security association. For instance, a combination of AH (transport mode) and ESP (tunnel mode) may assure confidentiality of the payload as well as data integrity of the whole IP packet including outer header. In such case, PF_KEY MIGRATE message may be used for updating endpoint addresses of IPsec transport mode.

4.1.6. NAT Traversal

TOC

Dual Stack Mobile IPv6 [I-D.ietf-mip6-nemo-v4traversal] (Soliman, H., “Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6),” November 2007.) supports a scenario where a MN is connected to a network behind a Network Address Translator (NAT). In such case, the MN assigns an IPv4 private address to its network interface but it is still capable of registering its care-of address to the HA, using the NAT Traversal technique [RFC3948] (Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, “UDP Encapsulation of IPsec ESP Packets,” January 2005.). The MN and HA leverage an IPsec tunnel to protect the return routability messages.
It is possible for the PF_KEY MIGRATE message to handle IPv4 private address when the MN is behind a NAT device. In a NAT Traversal case, the endpoint address of the MN is characterized by the IP address and the pair of source and destination port numbers used for the UDP encapsulation. Therefore, in a NAT Traversal scenario, a Mobile IPv6 module MUST issue a PF_KEY MIGRATE message along with the pair of source and destination port numbers of a UDP encapsulation, to handle IPv4 private address.

TOC

4.1.7. Limitation of PF_KEY MIGRATE

Currently, a Security Parameter Index (SPI) is not included in the old SA information to specify target SAD entry. This helps to lessen operational burden of Mobile IPv6. However, this simplification can produce ambiguity in searching for the target security association entry. When the unique SPD level is available, it should be used because it avoids this problem both by marking the SAs to update and by limiting SA sharing.
It should be noted that delivery of PF_KEY MIGRATE messages cannot be guaranteed, which is common to other PF_KEY messages. It may be possible that a MIGRATE message is lost. In such case, there will be inconsistency between the binding record managed by Mobile IPv6 and IPsec database inside the kernel or the IKE daemon. Once a PF_KEY MIGRATE message is lost, it would not be possible for the receiver to process some subsequent MIGRATE messages properly. Reinitialization of the Mobile IPv6 stack and IPsec databases may be needed for recovery.

4.1.8. Interoperability Issue

TOC

It is a choice of implementers whether to support the PF_KEY MIGRATE message in their MIPv6 and IPsec/IKE implementations. However, asymmetry in the support of the PF_KEY MIGRATE message may cause an interoperability issue in some case.
It should be noted that an interoperability issue may be raised when the HA does not support PF_KEY MIGRATE message whereas the MN does support the mechanism. This is based on the working assumption that HA serves as a responder in the IKE negotiations conducted to maintain the IPsec SAs required for MIPv6 operation. It is unlikely that the HA serves as an initiator in the IKE negotiation in the MIPv6 network scenario for practical reasons. Thus, the HA without the support of PF_KEY MIGRATE suffers from having the old information in the IPsec database. More specifically, the HA may forward the IP packets destined for the MN to a wrong destination.
Therefore, it is RECOMMENDED that HA implements PF_KEY MIGRATE message or equivalent function to avoid an interoperability issue with regard to the dynamic update of IPsec database.

4.2. PF_KEY Packet Extension

TOC

In the bootstrapping stage of Mobile IPv6, the MN and HA need to establish IPsec SA to protect signaling messages of Mobile IPv6 such as BU and BA. When IKE is used to establish and maintain the SA pairs, the

IKE negotiation is the very first transaction made between the MN and HA.
As mentioned in [RFC3776] (Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," June 2004.), a care is needed for the address management of the IKE negotiation in Mobile IPv6 environments. In particular, IKE negotiation to be made to establish a transport mode IPsec SA pair is tricky in a sense that the IKE endpoint and the SA address on the MN side are different; IKE endpoint must be an IP address other than the home address of the MN, whereas the SA address must be the MN's home address. This is because the home address cannot be used prior to the initial home registration. The best candidate for the IKE endpoint on MN side is the primary care-of address of the MN since it is verified by the Mobile IPv6 module to work.
For the above reasons, there is a need to guide IKE module to make the right choice of IKE endpoint and SA address. More specifically, IKE module should be notified on which IP address the IKE negotiation should run.
A simple solution which enables the notification is to add the information of the triggering packet to the SADB_ACQUIRE message. The extension is called Packet Extension, which allows a receiver of a SADB_ACQUIRE message (e.g. IKE module) to inspect the triggering packet and take necessary action, such as choosing specific IP address as an IKE endpoint for the subsequent IKE negotiation.
The following is a structure of an extended SADB_ACQUIRE message. As the figure shows, information of the triggering packet is appended to the SADB_ACQUIRE message.

```
     <base, address(SD), address(P)*, identity(SD)*,
                           sensitivity*, proposal, packet*>
```

4.2.1. Inserting Packet Extension to SADB_ACQUIRE Message

TOC

The IPsec subsystem MAY include a Packet Extension to a SADB_ACQUIRE message when absence of IPsec SA is detected during outbound packet processing. The IP packet to be included in the Packet Extension MUST be the very IP packet which triggered the ACQUIRE message IPsec sublayer.
The information of the triggering packet MUST contain IP header, IP header options (in the case of IPv4), IP extension headers (in the case of IPv6), and the transport layer protocol header if there is any.
More than one packet extensions MUST NOT be appended to a SADB_ACQUIRE message.
The figure below shows the format of the Packet Extension which conforms the extension header specified in [RFC2367] (McDonald, D.,

Metz, C., and B. Phan, “PF_KEY Key Management API, Version 2,” July 1998.).

```
struct sadb_x_packet {
        uint16_t sadb_packet_len;
        uint16_t sadb_packet_exttype;
        uint32_t sadb_packet_copylen;
};
/* sizeof(struct sadb_x_packet) == 8 */
/* followed by an IP packet header which triggered
                                the SADB_ACQUIRE message */
```

sadb_packet_copylen Indicates the exact length of the packet header that follows the extension header. Note that the 64 bit alignment rule applies to the Packet Extension thus there could be padding appended to meet the alignment requirement. This padding SHOULD be set to zero by the sender (kernel) and MUST be ignored by the receiver.

4.2.2. Extracting Home Registration Information from Acquire Message

TOC

A receiver of a SADB_ACQUIRE message with a Packet Extension MAY extract and process the extension header.
A Mobile IPv6 aware IKE daemon should be able to process a Packet Extension which includes the IPv6 packet containing the initial home registration BU message. An IPv6 packet which contains following information is suspected to be a home registration Binding Update message:

*A mobility header message with message type 5 (BU).

*In the BU message, Home Registration (H) bit is set.

The source address field of the IPv6 header is supposed to be the home address of the MN. In some systems, a home address destination option may be present in the IP packet. In such case, a care is needed to extract the care-of address of the MN. In any case, the care-of address MUST be extracted from the alternate care-of address, if the option is present in the packet.
Recommendation: Mobile IPv6 module is recommended to include an alternate care-of address option in every BU message, regardless of the

type of IPsec protocol (AH or ESP) which is used to protect the message.

4.2.3. Relation of Packet Extension to IKEv2

TOC

The Packet Extension is useful not only for Mobile IPv6 usage but also for other network scenarios where IKEv2 is used as a key management protocol.
In IKEv2 (Kaufman, C., "Internet Key Exchange (IKEv2) Protocol," December 2005.) [RFC4306], it is specified that the first traffic selector of TSi and TSr should contain the information of triggering packet when an initiator requests establishment of IPsec SA triggered by a data packet. The Packet Extension can provide the information of the triggering packet to the IKE module.

---

5. Necessary Modifications to Mobile IPv6 and IPsec/IKE

TOC

In order to realize the proposed mechanism, there are some necessary modifications to Mobile IPv6 and IPsec/IKE. Following are the summary of necessary modifications, which could be of interest to implementors of Mobile IPv6 and/or IPsec/IKE.

*Modifications to Mobile IPv6:

-The Mobile IPv6 code can make an access to PF_KEY socket. In particular, the Mobile IPv6 code should have privilege to write messages into a PF_KEY socket.

-Issuing PF_KEY MIGRATE messages: in order to send MIGRATE messages, it is required that the Mobile IPv6 code has some knowledge of its IPsec configuration and precise binding record. The Mobile IPv6 code may be aware of exact IPsec configuration in form or security policy. It would also be possible that the Mobile IPv6 code is only aware of minimum IPsec configuration whether if IPsec is utilized or not.

*Modifications to IPsec:

-Processing PF_KEY MIGRATE messages: the kernel should be able to process PF_KEY MIGRATE messages sent by the Mobile IPv6 code. Unless the message is invalid, it should be sent to all open PF_KEY sockets.

- Enabling Packet Extensions (SADB_X_EXT_PACKET): the kernel should be able to append a SADB_X_EXT_PACKET extension to SADB_ACQUIRE messages when they are triggered by an output of a data packet.

* Modifications to IKE:

- Processing PF_KEY MIGRATE messages: the IKE code may update its local copy of IPsec databases (SPD and SAD) in accordance with received PF_KEY MIGRATE messages. In addition, it may update its state / IKE session with new endpoint addresses indicated by PF_KEY MIGRATE messages.

- Processing of Packet Extensions (SADB_X_EXT_PACKET): the IKE code may process SADB_X_EXT_PACKET extensions and extract necessary information from triggering packets. In order for the IKE code to be MIPv6-aware, it should properly extract the home address, care-of address, and HA address from IP packets which carry home registration BU messages.

---

6. Security Considerations

TOC

The proposed schemes in this document do not raise any security issue with regard to the authenticity of the IP packets to be handled under the protection of an IPsec SA pair in tunnel mode. This is because authenticity of the IP packet has nothing to do with IP addresses in the IP header.

---

7. Conclusion

TOC

* There is a need for Mobile IPv6 and IPsec/IKE to interact with each other to provide full support of IPsec security functions.

* An extension to the PF_KEY framework (PF_KEY MIGRATE message) is proposed, which makes it possible for the IPsec/IKE to migrate an endpoint address of tunnel IPsec SAs from one to another.

* PF_KEY MIGRATE messages also make it possible for IKE to survive movements by updating its IKE session.

* In order for the IKE to perform key negotiations and rekeying, effort should be made to keep its SPD image up-to-date.

*The proposed mechanism was implemented on both Linux and BSD platforms and confirmed to be working well.

*Currently, large portion of the proposed mechanism is implementation dependent due to lack of standard interface to access the SPD (PF_POLICY?).

8. References

TOC

8.1. Normative References

TOC

[RFC2367]	McDonald, D., Metz, C., and B. Phan, "PF_KEY Key Management API, Version 2," RFC 2367, July 1998 (TXT).
[RFC2401]	Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, November 1998 (TXT).
[RFC2409]	Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409, November 1998 (TXT).
[RFC3775]	Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004 (TXT).
[RFC3776]	Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," RFC 3776, June 2004 (TXT).
[RFC4301]	Kent, S. and K. Seo, "Security Architecture for the Internet Protocol," RFC 4301, December 2005 (TXT).
[RFC4306]	Kaufman, C., "Internet Key Exchange (IKEv2) Protocol," RFC 4306, December 2005 (TXT).

8.2. Informative References

TOC

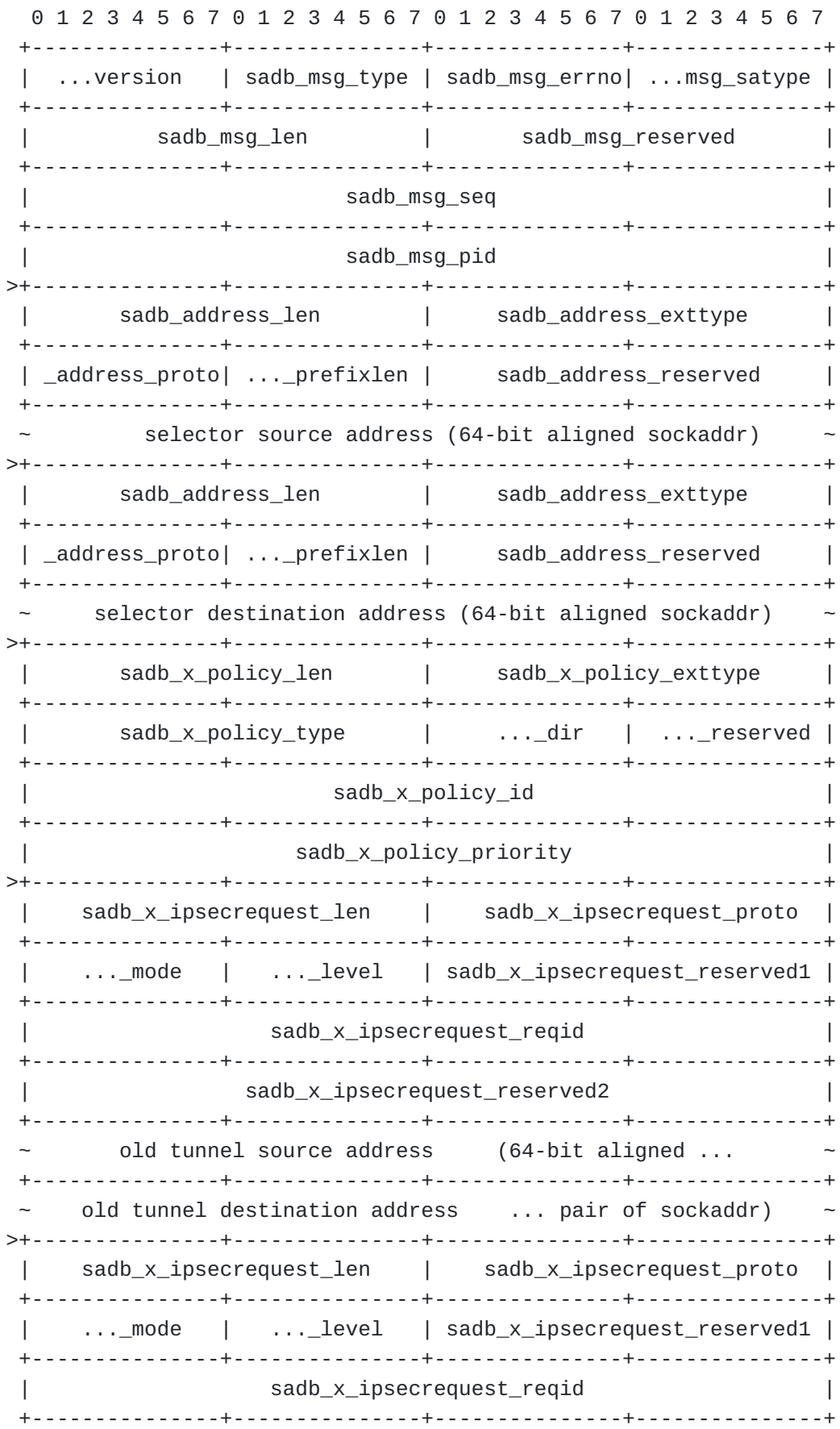
[I-D.ietf-hip-mm]	Henderson, T., "End-Host Mobility and Multihoming with the Host Identity Protocol," draft-ietf-hip-mm-05 (work in progress), March 2007 (TXT).
[I-D.ietf-mip6-nemo-v4traversal]	Soliman, H., "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)," draft-ietf-mip6-nemo-v4traversal-06 (work in progress), November 2007 (TXT).
[RFC3948]	Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets," RFC 3948, January 2005 (TXT).
[RFC3963]	

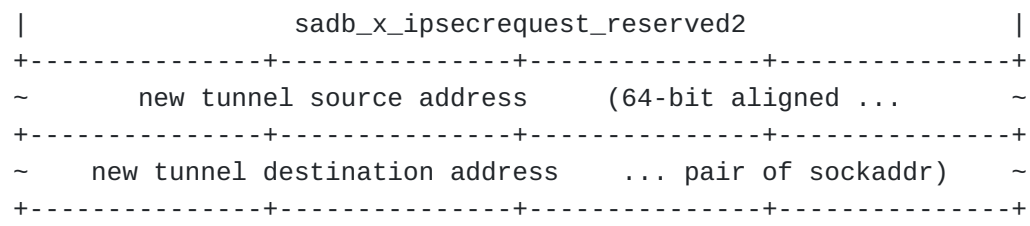
	Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, “Network Mobility (NEMO) Basic Support Protocol,” RFC 3963, January 2005 (TXT).

Appendix A. PF_KEY MIGRATE Message Format

TOC

The figure below shows the message format of PF_KEY MIGRATE. The message consists of 6 parts (boundary of each part is marked with ">"). The message starts with PF_KEY base message header followed by two address extensions. A pair of address extensions hold source and destination address of the selector. Rest of the message are specific to IPsec implementation on BSD. sadb_x_policy{} structure holds additional information of security policy. The last part of the message is a pair of sadb_x_ipsecrequest{} structures that hold old and new SA information.


0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
...version
sadb_msg_type
sadb_msg_errno
...msg_satype
sadb_msg_len
sadb_msg_reserved
sadb_msg_seq
sadb_msg_pid
sadb_address_len
sadb_address_exttype
_address_proto
..._prefixlen
sadb_address_reserved
selector source address (64-bit aligned sockaddr)
sadb_address_len
sadb_address_exttype
_address_proto
..._prefixlen
sadb_address_reserved
selector destination address (64-bit aligned sockaddr)
sadb_x_policy_len
sadb_x_policy_exttype
sadb_x_policy_type
..._dir
..._reserved
sadb_x_policy_id
sadb_x_policy_priority
sadb_x_ipsecrequest_len
sadb_x_ipsecrequest_proto
..._mode
..._level
sadb_x_ipsecrequest_reserved1
sadb_x_ipsecrequest_reqid
sadb_x_ipsecrequest_reserved2
old tunnel source address
(64-bit aligned ...
old tunnel destination address
... pair of sockaddr)
sadb_x_ipsecrequest_len
sadb_x_ipsecrequest_proto
..._mode
..._level
sadb_x_ipsecrequest_reserved1
sadb_x_ipsecrequest_reqid



Following is a structure of PF_KEY base message header specified in [RFC2367] (McDonald, D., Metz, C., and B. Phan, "PF_KEY Key Management API, Version 2," July 1998.). A new message type for PF_KEY MIGRATE (i.e., SADB_X_MIGRATE) should be specified in member sadb_msg_type.

```
struct sadb_msg {
        uint8_t         sadb_msg_version;
        uint8_t         sadb_msg_type;
        uint8_t         sadb_msg_errno;
        uint8_t         sadb_msg_satype;
        uint16_t        sadb_msg_len;
        uint16_t        sadb_msg_reserved;
        uint32_t        sadb_msg_seq;
        uint32_t        sadb_msg_pid;
};
```

Following is a structure of address extension header specified in [RFC2367] (McDonald, D., Metz, C., and B. Phan, "PF_KEY Key Management API, Version 2," July 1998.). Upper layer protocol should be specified in member sadb_address_proto.

```
struct sadb_address {
        uint16_t        sadb_address_len;
        uint16_t        sadb_address_exttype;
        uint8_t         sadb_address_proto;
        uint8_t         sadb_address_prefixlen;
        uint16_t        sadb_address_reserved;
};
```

Following is a structure for holding attributes that are relevant to security policy, which is available on BSD IPsec implementation. Direction of the target security policy should be specified in member sadb_x_policy_dir.

```
struct sadb_x_policy {
        uint16_t        sadb_x_policy_len;
        uint16_t        sadb_x_policy_exttype;
        uint16_t        sadb_x_policy_type;
        uint8_t         sadb_x_policy_dir;
        uint8_t         sadb_x_policy_reserved;
        uint32_t        sadb_x_policy_id;
        uint32_t        sadb_x_policy_priority;
};
```

Following is a structure for holding attributes that are relevant to security association, which is available on BSD IPsec implementation. IPsec protocol (ESP or AH) and mode (Tunnel) of the target security association should be provided in member sadb_x_ipsecrequest_proto and sadb_x_ipsecrequest_mode, respectively.

```
struct sadb_x_ipsecrequest {
        uint16_t        sadb_x_ipsecrequest_len;
        uint16_t        sadb_x_ipsecrequest_proto;
        uint8_t         sadb_x_ipsecrequest_mode;
        uint8_t         sadb_x_ipsecrequest_level;
        uint16_t        sadb_x_ipsecrequest_reserved1;
        uint32_t        sadb_x_ipsecrequest_reqid;
        uint32_t        sadb_x_ipsecrequest_reserved2;
};
```

Appendix B. Acknowledgements

TOC

The authors gratefully acknowledge the contribution of (in alphabetical order): Arnaud Ebalard, Sebastien Decugis, Mitsuru Kanda, Kazunori Miyazawa, Tsuyoshi Momose Shoichi Sakane, Keiichi Shima, Noriaki Takamiya, and Hideaki Yoshifuji.
Support of NAT Traversal was suggested by Kazunori Miyazawa.
Kazunori Miyazawa provided valuable comments on Packet Extension.
Arnaud Ebalard provided valuable comments on Packet Extension based on his implementation experience.
This document was generated by xml2rfc.

Authors' Addresses

TOC

	Shinta Sugimoto
	Nippon Ericsson K.K.
	Koraku Mori Building

	1-4-14, Koraku, Bunkyo-ku
	Tokyo 112-0004
	Japan
Phone:	+81 3 3830 2241
Email:	shinta.sugimoto@ericsson.com
	Francis Dupont
	CELAR
Email:	Francis.Dupont@fdupont.fr
	Masahide Nakamura
	Hitachi Communication Technologies, Ltd.
	216 Totsuka-cho, Totsuka-ku
	Yokohama 244-8567
	Japan
Phone:	+81 45 865 7003
Email:	masahide.nakamura.cz@hitachi.com

Full Copyright Statement

TOC

Intellectual Property

can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.
The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.