Recommended Paper

Interactions between Mobile IPv6 and IPsec/IKE

Shinta Sugimoto,† Francis Dupont†† and Ryoji Kato†

We specified a mechanism with which Mobile IPv6 and IPsec/IKE can work together efficiently. The interaction is necessary for updating the endpoint address of an IPsec tunnel in accordance with movement performed by a mobile node. Based on an analysis of needs for interaction between Mobile IPv6 and IPsec/IKE, we designed and implemented a mechanism that is an extension to the PF_KEY framework. The proposed mechanism allows Mobile IPv6 to inform IPsec/IKE of the movement so that necessary updates to the security policy database and security association database can be taken by IPsec/IKE. This notification helps IKE to update its internal state. The mechanism is also applicable to the other scenarios, such as NEMO, Mobile VPN and its variants.

1. Introduction

Mobile IPv6 [1] is a protocol that provides mobility support for IPv6. In Mobile IPv6, an intelligent router called a home agent works as a routing anchor for the mobile nodes. The home agent maintains binding of a permanent identifier and a locator for each mobile node in a database called a *Binding Cache*. The identifiers and locators are in form of IPv6 addresses, and they are called *home addresses* and *care-of addresses*, respectively. An IP packet destined for the home address of a mobile node is intercepted by the home agent and forwarded to the current location of the mobile node, namely the care-of address. Mobile IPv6 relies on IPsec [2] to secure the protocol operation [3], because it is essentially an extension to the IP layer, and the mobility signals are sent over the IP networks. In Mobile IPv6, mobile users can additionally leverage IPsec tunnels to secure user data.

A virtual private network (VPN) is a network that is constructed virtually on the public Internet. A VPN provides secure access to remote network by using an authentication mechanism and cryptographic technologies. Only authorized users are able to access a VPN. The most typical VPN scenario is when a mobile client establishes an IPsec tunnel with its security gateway and traverses all traffic through it. This scenario is called Mobile VPN. An IPsec tunnel is beneficial for mobile users to protect sensitive data, such as classified documents or on-line payment information. Specifically in a wireless environment, users risk having their data eavesdropped by malicious third parties that may tap into the link.

Both in Mobile IPv6 and Mobile VPN scenarios, movement of the client affects the IPsec tunnel as the outer IP header should contain topologically correct IP addresses. That is, the endpoint address of the IPsec tunnel on the client side should be updated when it changes its attachment point to the Internet. As a consequence of address updating, security policy database (SPD) and security association database (SADB) should be correctly updated. The address updating can be done by re-establishing security associations between the peers. However, this is not desirable because of latency and signaling costs caused by Internet key exchange (IKE).

Our objective is to solve this problem by specifying a mechanism that enables interaction between Mobile IPv6 and IPsec/IKE. Our proposed mechanism allows Mobile IPv6 to inform IPsec/IKE of movements so that address updating can be performed without re-establishing the security associations. The mechanism extends PF_KEY framework [4]. By receiving the notification from Mobile IPv6, IPsec/IKE can take necessary updates to the SPD and SADB. The notification can also be used by IKE to maintain its connection to peers.

In Section 2, we present a security model of

† Nippon Ericsson K.K., Ericsson Research Japan
†† Networks and Multimedia Research Department of GET/ENST Bretagne

The initial version of this paper was presented at the 31st SIG conference of MBL held on Nov. 2004 sponsored by SIGMBL and SIGITS, whose proceedings are IPSJ SIG Technical Reports 2004-MBL-31. This paper was recommended to be submitted to IPSJ Journal by the chairman of SIGMBL.

Mobile IPv6 and potential threats to it. In Section 3, we analyze the needs for interaction between Mobile IPv6 and IPsec/IKE. In Sections 4 and 5, we present the design and prototype implementation of our proposed mechanism, respectively. In Section 6, we discuss the applicability of our proposed mechanism to other scenarios.

2. Security in Mobile IPv6

In this section, we introduce the security model in Mobile IPv6 along with potential threats and rationale behind the protocol design. Then we focus on the significance of the IPsec tunnel from the protocol operation viewpoint and the user perspective.

2.1 Security Threats in Mobile IPv6

Mobile IPv6 was designed to not lower the security level of the existing Internet, and care was taken to prevent the protocol from imposing any security threats [5]. By nature, Mobile IPv6 has the potential to impose security holes because it specifies exceptional handling in IP routing: to re-direct traffic destined to a particular IP address that is registered in a binding cache database. Hence, maintaining correct binding information is crucial. Proper authentication and authorization should be made when creating or updating the binding information at a home agent and correspondent nodes. In particular, the binding cache maintained by the home agent must be secured because it serves as a constant routing anchor for the mobile nodes. If the home agent accepts false binding registration, the home agent itself could become a stepping stone for launching reflection attacks.

2.2 Security Model and Assumptions

The security model in Mobile IPv6 is based on the assumption that a strong trust relationship exists between a mobile node and its home agent while a weak trust relationship exists between the mobile node and its correspondent. The security model and the paths that user traffic can take are illustrated in **Fig. 1**. Given the assumption, Mobile IPv6 specifies how to apply IPsec [2] to protect mobility signals exchanged between the home agent and mobile node. The binding update and binding acknowledge messages are protected by the transport mode IPsec. A different security mechanism is specified for correspondent registration, which is called the return routability procedure. Optionally, IPsec could be applied to the mobility signals sent between the mobile node and correspondent node if security association is in place [6]. The purposes of the return routability procedure are verification of the reachability of the mobile node with the claimed addresses, namely the home address and the care-of address, and generation of a symmetric key called *binding management key (Kbm)* for the mobile node and correspondent node to authenticate and authorize the binding update message. The return routability procedure includes two types of message exchanges called a *home test* and *care-of test*.

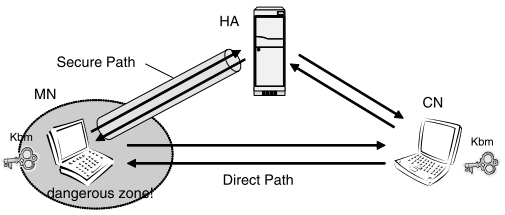

Fig. 1 Security model in Mobile IPv6.

A home test is initiated by the mobile node by sending a challenge message called home test init (HoTI) to the correspondent node. If the challenge is received by the correspondent node, the node replies with a response message called home test (HoT). A HoT message includes a cryptographically generated token, called a home keygen token. HoTIs and HoTs are sent over the secure path as described in Fig. 1. The care-of test procedure is basically the same as home test procedure, except for the path that messages take. While care-of test messages are directly exchanged, home test messages are exchanged through the home agent. In particular, home test messages must be protected by an IPsec tunnel with ESP encapsulation to prevent malicious third parties from eavesdropping the contents of the return routability procedure. That is, an attacker cannot impersonate a mobile node unless it is sitting on a path between the home agent and correspondent node. This design choice is based on an assumption that a mobile node is potentially more exposed to danger in its visiting network [5]. Kbm is generated from the home and care-of keygen tokens and is used by the correspondent node to verify if the received binding update message was sent by the node with whom the return routability procedure had been performed.

2.3 Key Management Scenarios

The IPsec security association required for Mobile IPv6 operation can be managed by either manual keying or dynamic keying. The

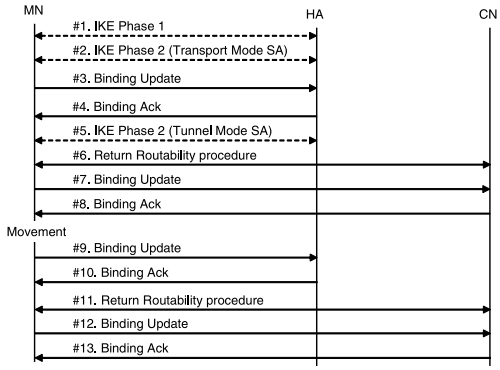

Fig. 2 Message sequence of Mobile IPv6 with IKE.

security association includes keying materials and additional information. In manual keying, the operator of a home agent must configure security parameters for each mobile node statically. In dynamic keying, IKE can be used to establish and maintain IPsec security associations. In Mobile IPv6, IKE runs on the mobile node and home agent in order to establish IPsec security associations. The major advantages of dynamic keying over manual keying are the reduction of operational costs and anti-replay protection. Making static configuration for may mobile nodes would be neither practical nor efficient. Manual keying is vulnerable to replay attacks. With IKE, the initiator and responder can take advantage of the anti-replay protection provided by ESP and AH. Note that Mobile IPv6 signaling message has a sequence number but it cannot provide complete anti-replay protection. Hence, dynamic keying is more cost-effective and scalable.

A message sequence of Mobile IPv6 signaling along with IKEv1 negotiations is illustrated in **Fig. 2**. In the initial stage, the mobile node and home agent must establish IPsec security association in transport mode which is necessary for protecting home registration messages (#1 and #2 in the Fig. 2). When the security association becomes available, home registration is performed (#3 and #4). In this scenario, the mobile node tries to perform correspondent registration after home registration. Prior to the return routability procedure, an IPsec tunnel should be established between the mobile node and home agent. Another IKE Phase-2 negotiation is performed to establish IPsec security association in tunnel mode (#5). Accordingly, the return routability procedure takes place (#6). Note that the IPsec tunnel is used to carry home test messages. Finally, correspondent registration is done (#7 and #8). Upon movement, the mobile node performs home registration followed by correspondent registration. A return routability procedure (care-of test) is required before correspondent registration.

3. Requirements

In this section, we address a series of requirements that should be fulfilled for Mobile IPv6 and IPsec/IKE to work together smoothly.

1) Updating Tunnel Endpoints

First, consider how to update endpoint addresses of IPsec tunnels upon movement of the mobile node. Mobile IPv6 does not specify how the address updating should be done. One alternative is re-establishing IPsec security association per movement. However, this is not desirable in terms of latency and signaling overhead. The IKE negotiation would run on a new care-of address, and consequently, the endpoint address of the security association should be updated accordingly. In the case of IKEv1, the initiator (mobile node) and responder (home agent) should perform Phase-2 IKE negotiation, which has a 1.5 round trip time. From the IPsec perspective, the endpoint addresses of IPsec tunnels are stored in the SPD and SADB. In the case of Mobile IPv6, the endpoint address on the client side should be the primary care-of address of the mobile node, which can only be determined by Mobile IPv6. Therefore, a need exists for Mobile IPv6 to notify the movement and inform IPsec/IKE of the new care-of address.

2) Performance Optimization of IKE

Second, concern exists about the survivability of an IKE connection upon movement of mobile node. In IKE, the initiator and responder establish a session and maintain the state. The session is protected by a session key, which is generated from the Diffie-Helman key exchange. In normal cases, IKE connectivity may not survive when the IKE peer changes the IP address used for IKE negotiation, which will end up re-establishing the IKE connection for each movement. To avoid this, Mobile IPv6 can guide IKE components to migrate the IKE connection according to the movement. This optimization is defined in Mobile IPv6, and the feature is called key management capability, which is indicated in a flag in a binding update message. Although, no mechanism exists that specifies how this feature is supported.

3) Dynamic Access to the SPD
Third, we identified the necessity for dynamically updating the SPD in Mobile IPv6 operation with IPsec. While the IPsec tunnel should be kept active when the mobile node is visiting foreign networks, the tunnel should be torn down when the mobile node stays at home. Therefore, the SPD must be updated in accordance with the movement; an SPD entry should be added when the mobile node moves from the home network to a foreign network, and SPD entries should be deleted when the mobile node returns home.

4. Design

In this section, we present the design of a mechanism that enables interaction between Mobile IPv6 and IPsec/IKE. Our proposed mechanism is an extension of the PF_KEY framework.

4.1 Design Goals

The followings are the design goals we set:

- Specification of a mechanism with less dependency on implementation or platform.
- Minimization of necessary modifications. Specifically, the changes required to IPsec should be kept to a minimum, as the requirements are raised by Mobile IPv6.
- Ensuring the mechanism is robust and will continue to work even if either the mobile node and home agent are rebooted during the sequence.

4.2 Extension to the PF_KEY Framework

Given the requirements stated in Section 3, we initially designed an interface between Mobile IPv6 and IPsec/IKE by extending the routing socket [7]. A new routing socket message named RTM_MOVEMENT was introduced. Mobile IPv6 issues the message to the routing socket when a movement takes place. However, the mechanism does not not fully accomplish the design goals stated earlier; the routing socket was originally an interface for the routing layer and is available on BSD systems, and the mechanism requires relatively large changes to IPsec/IKE. Thus, we continued seeking a better solution for the mechanism and reached the conclusion that the PF_KEY framework [4] is more suitable for the interface between the Mobile IPv6 and IPsec/IKE [8]. This design choice was made to fulfill the first and second design goals. The PF_KEY framework is an interface to the IPsec database and is available on various platforms. IPsec/IKE are by definition familiar with the PF_KEY framework.

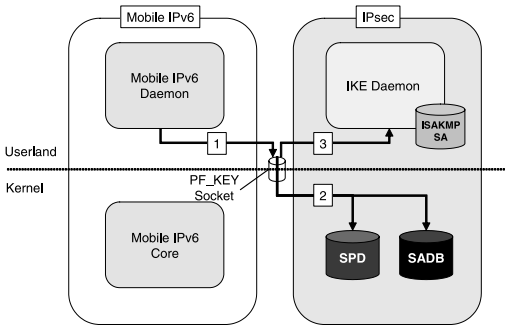

Fig. 3 System overview.

4.3 PF_KEY MIGRATE Message

We introduced a new PF_KEY message named MIGRATE is introduced, which is used by Mobile IPv6 components to notify other system components of movement asynchronously. The message is issued whenever the primary care-of address of the mobile node is changed. The message is used on both the mobile node and home agent. On a mobile node, the MIGRATE message is issued when the primary care-of address is changed. On a home agent, the MIGRATE message is issued when the home registration indicates that primary care-of address of the mobile node has been changed.

A system overview is shown in **Fig. 3**. As the figure shows, a PF_KEY socket works as an intermediate service for Mobile IPv6 and IPsec/IKE. On the left, Mobile IPv6 components are divided into two pieces, the daemon and the core. On the right are IPsec components, the IKE daemon, and the IPsec core.

On mobile node, the following steps are taken when movement is performed:

(i) The Mobile IPv6 core detects movement and performs home registration.
(ii) The Mobile IPv6 daemon announces movement to the system by issuing a PF_KEY MIGRATE message (arrow #1 in Fig. 3).
(iii) The kernel receives and verifies the message. If it is acceptable, the IPsec core inside the kernel takes the necessary update to the SPD and SADB (arrow #2). Accordingly, the message is broadcasted to all open PF_KEY sockets (arrow #3).
(iv) The PF_KEY MIGRATE message is received by the IKE daemon, and endpoint addresses stored in the local copy of the

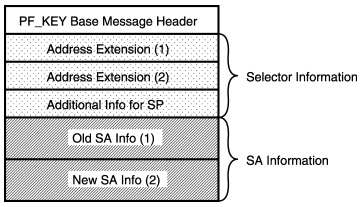

Fig. 4 Header format of PF_KEY MIGRATE message.

SPD and SADB (if any) are updated according to the message. IKE connection is also updated if necessary.

With regard to the procedures taken on the home agent, the steps are almost identical to those in the mobile node case except that the migration is initiated by the home registration. When the home agent receives a binding update message indicating that the primary care-of address of the mobile node has been changed, address updating procedure is invoked and following steps (ii) to (iv) are taken.

The header format of a PF_KEY MIGRATE message is illustrated in **Fig. 4**. The message is threefold: a PF_KEY base message header, selector information, and security association information. The selector information part contains a pair of address extension headers and the additional information. The address extension headers contain source and destination addresses of the selector information. The contents of the selector information part are used for identifying the target security policy entry to be updated. Next comes the security association information part, which contains a pair of SA Info. SA Info is a data structure which contains a set of SA parameters. The first SA Info contains parameters of the old SA Info from which one can learn the old tunnel endpoints. The new SA Info contains new endpoints of the tunnel. The address pair included in the SA Info is the most essential part of the message in the sense that it tells the old and new endpoint addresses.

4.3.1 Necessary Modifications

The following is a summary of the necessary modifications to Mobile IPv6, IPsec, and IKE required by our proposed mechanism:

- Modifications to Mobile IPv6

Mobile IPv6 must be modified so that it can access the PF_KEY socket to issue the MIGRATE message. In addition, a Mobile IPv6 component must have enough knowledge of IPsec configuration, which is relevant to Mobile IPv6 protocol operation. In particular, the configuration should be in the form of security policy. However, Mobile IPv6 is not required to have specific knowledge of security associations such as encryption and authentication algorithms and keys.

- Modifications to IPsec

The IPsec stack inside the kernel must be modified so that it can process the MIGRATE message issued by Mobile IPv6. Necessary updates should be made on SPD and SADB according to the MIGRATE message. The target SPD entry is specified by the selector information stored in the MIGRATE message. Accordingly, updating of the tunnel endpoint address in SADB should be made. The target SADB entry should be the one which is associated with the target SPD entry.

- Modifications to IKE

IKE must be modified so that it can process the MIGRATE message and update its local copy of SPD and SADB. In addition, IKE can update the endpoint of the IKE connection with its peer according to the MIGRATE message, which makes the IKE mobility-aware.

5. Prototype Implementation

Based on the design presented in Section 4, we implemented the PF_KEY extension on Linux-2.6. The changes we made to the existing software were the functions stated in Section 4.3.1. We implemented the proposed mechanism on MIPL2.0, which is an open source Mobile IPv6 stack called MIPL2.0 [9]. MIPL2.0 was jointly developed by Helsinki University of Technology (HUT) GO/Core Project and USAGI Project [10]. Our proposed mechanism was incorporated in the latest software release in MIPL2.0. The userland daemon is called `mip6d` issues the MIGRATE message to the PF_KEY socket when the mobile node moves. For the IKEv1 daemon, we used an open source software called `racoon`. `racoon` was originally developed by KAME Project [11] and is currently maintained by ipsec-tools project [12]. To make the IKE daemon mobility-aware, we defined two functions named `updateph1()_remote` and `updateph1_local()`, which are for updating the endpoints of the IKE connection on the mobile node and home agent, respectively.

With the prototype implementation, we verified whether our proposed mechanism fulfilled all the requirements given in Section 3. We confirmed that the system successfully worked both

in static keying and dynamic keying scenarios. Our proposed mechanism could handle all types of movement, Home-to-Foreign, Foreign-to-Foreign, Foreign-to-Home, and we confirmed that SPD and SADB, as well as internal state of IKE were correctly updated. Also, the system was not affected even if either the mobile node or the home agent is rebooted.

6. Analysis and Discussions

In this section, we discuss and analyze the PF_KEY MIGRATE message in detail. In particular, we consider the applicability and the implications of the design of the PF_KEY MIGRATE message for the IPsec architecture.

6.1 Applicability to Mobile VPN

MOBIKE[13] is an extension to IKEv2[14] that adds support for mobility and multihoming. With MOBIKE, the initiator and responder exchange sets of available endpoint addresses, and the initiator can inform the responder about changes of endpoint address without re-establishing security associations. A typical scenario is mobility (known as road-warrior), where a client roams around the networks changing its attachment point to the Internet. In such a case, the client changes its attachment point to the Internet in the same way as mobile node in Mobile IPv6. Hence, MOBIKE could be another usecase for PF_KEY MIGRATE messages.

A sequence of address updates as well as processing of a PF_KEY MIGRATE message is depicted in **Fig. 5**. In this figure, it is assumed that the initiator and responder have established IPsec security association prior to the address updating. Suppose the initiator changes its local address from *I1* to *I2*. When the initiator detects that *I1* is no longer available and wishes to switch to another address, *I2*, it sends an INFORMATIONAL request message, which contains UPDATE_SA_ADDRESS notification payload telling its new address, *I2*. The initiator then issues a MIGRATE message and the address is updated. When the responder receives the message requesting for address updating, it verifies whether the initiator requested a valid IP address either by using a certificate or a return routability check. Once the IP address is confirmed to be valid, the responder takes the address update by issuing the MIGRATE message.

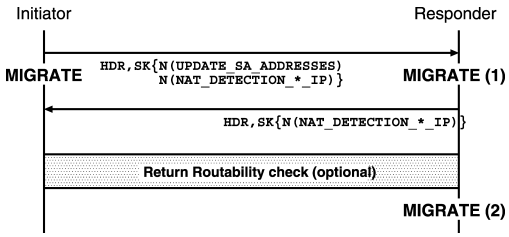

Fig. 5 Updating SA address in MOBIKE.

Hence, our proposed mechanism is applicable for MOBIKE. Both initiators and responders can use the MIGRATE message to update endpoint addresses of the IPsec tunnels.

6.2 Applicability to IPv4/IPv6 Environment

Next, we considered the case where an IP address family is incompatible between the IP subnets that the mobile node visits. During the transition phase from IPv4 to IPv6, the Internet will be a mixture of IPv4 networks, IPv6 networks, and dual-stack networks. In such an environment, a transition mechanism may be needed. For instance, a node may not be able to send/receive IPv6 packets when it is attached to an IPv4 network. In such a case, the node may be bound to establish a transition tunnel to traverse traffic over the local network. Taking mobility and security into account, more tunneling will be required, which is not desirable in terms of multiple header overhead and sub-optimal routing. IPsec architecture is flexible enough to support IPsec tunneling in which IP address families of inner and outer IP headers are different; IPv4-in-IPv6 or IPv6-in-IPv4 IPsec tunneling. Therefore, using IPv4-in-IPv6 or IPv6-in-IPv4 IPsec tunnels to fulfill multiple requirements (security, mobility, and transition) is reasonable.

A scenario where a mobile VPN client performs movement from an IPv4 network to an IPv6 network is depicted in **Fig. 6**. As the figure shows, the IPsec tunnel should be switched from IPv4 to IPv6. Two main approaches exist for seamlessly moving a node from one IP subnet to another by adopting the address family incompatibility. In either case, we assumed that the client is aware of the IPv4 and IPv6 addresses of the security gateway.

In the first approach, a VPN client and a security gateway establish two pairs of security associations; one is IPv4-based, and the other is IPv6-based. The client updates its local address, which is an endpoint address of the IPsec tunnel when crossing the address family boundary. The security policy entry to be applied to

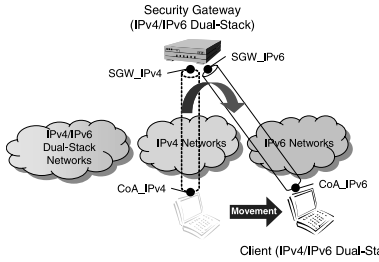

Fig. 6 Handover crossing over address family boundary.

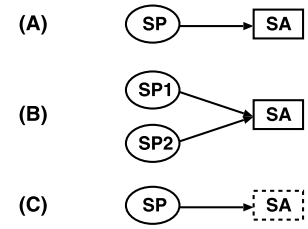

Fig. 7 Association of SPD entry and SA entry.

the user traffic should be associated with the tunnel mode security association entry, which is currently available. Thus, the association should be correctly updated in accordance with the movement.

In the second approach, a single security association pair in tunnel mode is established between the client and security gateway. When the client moves across the address family boundary, the address updating takes place. Both local and remote endpoints are updated during the address update. In the case of Fig. 6, the tunnel endpoints are updated from ⟨*CoA_IPv4, SGW_IPv4*⟩ to ⟨*CoA_IPv6, SGW_IPv6*⟩.

We believe that a PF_KEY MIGRATE message can handle both these cases. However, the first approach is complex in the sense that it requires dynamic updating of the linkage between security policy and security association. Hence, we believe that the second approach is more steadier.

6.3 Applicability to NEMO Basic Support

NEMO basic support [16] is an extension to the Mobile IPv6 to support mobility for a network. In NEMO, a mobile router changes its attachment point to the Internet; the network moves as a whole. A network prefix assigned to the mobile router is called a mobile network prefix (MNP), and nodes inside the mobile network uses IP addresses that are derived from the MNP. Traffic between the nodes inside the mobile network and the Internet is sent over the bi-directional tunnel established between the mobile router and its home agent. Optionally, a mobile router can use an IPsec tunnel to protect user traffic. In such a case, the mobile router and home agent should properly manage SPD and SADB according to the movement of the mobile router. Our proposed mechanism can be applied to NEMO basic support in the same way as Mobile IPv6.

6.4 Implications for IPsec Architecture

A PF_KEY MIGRATE message is designed in a way that the message is issued for each security policy. In other words, updating of endpoint addresses is primarily taken on SPD. Accordingly, if any tunnel mode entry exists in SADB that is associated with the security policy entry, the endpoint address is updated. This design choice is based on a conceptual model of association between security policy and security association. Three variants of associations are illustrated in **Fig. 7**. In scenario (A), the SPD entry and SA entry are in one-on-one association. In scenario (B), conceptually the target SADB entry is associated with multiple SPD entries. In scenario (C), the association is one-on-one, however, no SADB entry exists yet. This is possible in some scenarios where security association is dynamically created by IKE negotiation when needed. PF_KEY MIGRATE should properly work in any of these cases.

A PF_KEY MIGRATE message is a feature for updating endpoint addresses of the IPsec tunnels, which is a commonly required function in mobile environments. When addresses are updated, both the SPD and SADB should be affected. From an IPsec architecture perspective, the address updating has a potential effect on identification of SADB entries. The traditional IPsec architecture [2] specifies that inbound a given SADB entry should be uniquely identified with ⟨*destination IP address, security parameter index (SPI), and IPsec protocol*⟩ tuple for incoming packets. As a consequence of PF_KEY MIGRATE, the endpoint address stored in an SADB entry is changed. That is, the key information for identifying the inbound SADB entry might be changed. In Mobile IPv6, the inbound SADB entry maintained by the mobile node should be the case. As mentioned earlier, some form of linkage should exist from an SPD entry to an SADB entry. In a sys-

tem where the "linkage" occurs by the tuple to identify an SADB entry, care should be made to avoid affecting the address updating. Linkage between the SPD entry and SADB entry should be maintained in a stable manner. In the new IPsec architecture [17], an inbound SADB entry should be uniquely identified by an SPI.

7. Related Works

Schilcher, et al. proposed an extension to the PF_KEY framework that is necessary for MOBIKE [15]. In their proposal, a set of extensions to the PF_KEY framework are defined, including the feature to update the endpoints in the SADB. Although both of the mechanisms proposed here and in Schilcher's proposal aim to achieve a similar goal, a significant different exists.

In Schilcher's proposal, the SPI is used to identify the target SADB entry of the address updating. Access to SPI, which is specific information managed by IPsec/IKE, should be easy for MOBIKE components but not for Mobile IPv6 components. Moreover, SPI can be updated whenever the security association is rekeyed. Thus, having Mobile IPv6 components keep track of the SPI of a given security association is not feasible. In our proposal, the target SPD entry is searched for by a traffic selector, which should not be difficult for the Mobile IPv6 components to generate based on the security configuration. We assumed that the Mobile IPv6 components are aware of the security configuration that is required for the operation.

Also, in our proposal, address updating is performed primarily on the SPD, as stated in Section 6.4. The design choice assures that endpoints stored in a given SPD entry and its associated SADB entry are always consistent. In Mobile IPv6, an SPD entry that invokes the establishment of the tunnel mode IPsec security association must store correct IP address pair, namely the home agent address and the care-of address of the mobile node. In subsequent key negotiation, the IKE can extract the endpoint IP addresses from the SPD entry and set them as the endpoints of the newly created IPsec security association. In this way, address selection of the endpoints of the IPsec tunnel can be done more precisely, rather than implicitly taking the IP address pair used during the IKE negotiation.

From these reasons, we believe that our proposal is more suitable for the interactions between Mobile IPv6 and IPsec/IKE.

8. Conclusion

We proposed a mechanism for Mobile IPv6 and IPsec/IKE to work together efficiently. The mechanism is essential for updating the endpoint address of an IPsec tunnel, which is a common requirement for Mobile IPv6 and Mobile VPN environments. We made an extension to PF_KEY framework introducing a new message called MIGRATE. Mobile IPv6 issues the message to notify movement to other protocol components, such as IPsec/IKE. By receiving the message, IPsec/IKE can update the endpoint address stored in the SPD and SADB without re-establishing a security association. Our proposed mechanism also allows IKE to maintain a connection with its peer. We implemented our proposed mechanism on Linux and confirmed that it fulfilled the requirements.

Our proposed mechanism is not only applicable to Mobile IPv6 but also to other systems where the endpoint of an IPsec tunnel must to be updated. We showed how MOBIKE can work with the assistance of a PF_KEY MIGRATE message. We also confirmed that the mechanism is flexible enough to handle handover crossing over the address family boundary.

Acknowledgments We would like to thank the members of the USAGI Project for providing valuable comments. We would like to acknowledge the contribution made by Masahide Nakamura in the development of an IPsec stack inside the Linux-2.6 kernel. Also, we are grateful for anonymous reviewers for providing thoughtful comments. Lastly, we would like to thank the ABC:EMMA Project members of Ericsson Research for supporting this work.

References

1) Johnson, D., Perkins, C. and Arkko, J.: Mobility Support for IPv6, RFC 3775, Internet Engineering Task Force (June 2004).
2) Kent, S. and Atkinson, R.: Security Architecture for the Internet Protocol, RFC 2401, Internet Engineering Task Force (Nov. 1998).
3) Arkko, J., Devarapalli, V. and Dupont, F.: Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, RFC 3776, Internet Engineering Task Force (June 2004).
4) McDonald, D., Metz, C. and Phan, B.:

PF_KEY Key Management API, Version 2, RFC 2367, Internet Engineering Task Force (July 1998).
5) Nikander, P., Arkko, J., Aura, T., Montenegro, G. and Nordmark, E.: Mobile IP version 6 Route Optimization Security Design Background, RFC 4225, Internet Engineering Task Force (Dec. 2005).
6) Dupont, F. and Combes, J.: Using IPsec between Mobile and Correspndent IPv6 Nodes, draft-ietf-mip6-cn-ipsec-02.txt, Internet Engineering Task Force, work-in-progress.
7) Sugimoto, S. and Kato, R.: Considerations of Interactions between Mobile IPv6 and IPsec/IKE, IPSJ MBL-18 Technical Report (Nov. 2004).
8) Sugimoto, S., Dupont, F. and Nakamura, M.: PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE, draft-sugimoto-pfkey-migrate-01.txt, Internet Engineering Task Force, work-in-progress.
9) MIPL Mobile IPv6, work-in-progress. http://www.mobile-ipv6.org
10) USAGI Project, work-in-progress. http://www.linux-ipv6.org
11) KAME Project, work-in-progress. http://www.kame.net
12) IPsec Tools, work-in-progress. http://ipsec-tools.sourceforge.net/
13) Eronen, P., et al.: IKEv2 Mobility and Multihoming Protocol (MOBIKE), draft-ietf-mobike-protocol-05.txt, Internet Engineering Task Force (Oct. 2005).
14) Kaufman, C., et al.: Internet Key Exchange (IKEv2) Protocol, RFC 4306, Internet Engineering Task Force (Dec. 2005).
15) Schilcher, U., Tschofenig, H. and Muenz, F.: MOBIKE Extensions for PF_KEY, draft-schilcher-mobike-pfkey-extension-01.txt, Internet Engineering Task Force, work-in-progress.
16) Devarapalli, V., Wakikawa, R., Petrescu, A. and Thubert, P.: Network Mobility (NEMO) Basic Support Protocol, RFC 3963, Internet Engineering Task Force (Jan. 2005).
17) Kent, S. and Seo, K.: Security Architecture for the Internet Protocol, RFC 4301, Internet Engineering Task Force (Dec. 2005).

(Received September 16, 2005)
(Accepted September 14, 2006)
(Online version of this article can be found in the IPSJ Digital Courier, Vol.2, pp.635–643.)

Editor's Recommendation

This paper proposed a new framework to inform IPsec/IKE the mobility information of MIPv6 based on the PF_KEY framework. The authors clarify through implementations the interaction between Mobile IPv6 and IPsec/IKE to show that it is necessary for them to update the endpoint address of the IPsec tunnel due to terminals mobility. The proposed framework is also applied to other two different keys exchange scenarios. The achievement of the paper gives a significant contribution to the further development of the future mobile computing with Mobile IPv6.

(Chairman of SIGMBL Takashi Watanabe)

Shinta Sugimoto received his M.A. degree in Media and Governance from Keio University in 2001. He has been working for Nippon Ericsson K.K. since 2001 and engaged in research on IP mobility and security in mobile systems. He joined the USAGI Project in 2005 January and has been involved in development of Mobile IPv6 implementation on Linux-2.6. He is a member of IPSJ, IEEE, and ACM.

Francis Dupont is the main author of one of the first IPv6 implementations as a researcher at INRIA. He studied at the École Polytechnique (1981 class) and received a Doctorat ès Sciences in 1990. GET/ENST Bretagne (a Telecom Engineer School in Brittany in France).

Ryoji Kato received an M.S. degree in information processing from Osaka University in 1991. He is currently a senior research engineer at Nippon Ericsson K.K. He has over 10 years of experience in the Internet and the telecommunications industry. His current research interests include authentication and security mechanisms in mobile networks.