Network Working Group
Request for Comments: 3776
Category: Standards Track

J. Arkko
Ericsson
V. Devarapalli
Nokia Research Center
F. Dupont
GET/ENST Bretagne

June 2004

Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents

Status of this Memo

Copyright Notice

Abstract

Mobile IPv6 uses IPsec to protect signaling between the home agent and the mobile node. Mobile IPv6 base document defines the main requirements these nodes must follow. This document discusses these requirements in more depth, illustrates the used packet formats, describes suitable configuration procedures, and shows how implementations can process the packets in the right order.

Table of Contents

1. Introduction

This document illustrates the use of IPsec in securing Mobile IPv6 [7] traffic between mobile nodes and home agents. In Mobile IPv6, a mobile node is always expected to be addressable at its home address, whether it is currently attached to its home link or is away from home. The "home address" is an IP address assigned to the mobile node within its home subnet prefix on its home link. While a mobile node is at home, packets addressed to its home address are routed to the mobile node's home link.

While a mobile node is attached to some foreign link away from home, it is also addressable at a care-of address. A care-of address is an IP address associated with a mobile node that has a subnet prefix from a particular foreign link. The association between a mobile node's home address and care-of address is known as a "binding" for the mobile node. While away from home, a mobile node registers its primary care-of address with a router on its home link, requesting this router to function as the "home agent" for the mobile node. The mobile node performs this binding registration by sending a "Binding Update" message to the home agent. The home agent replies to the mobile node by returning a "Binding Acknowledgement" message.

Any other nodes communicating with a mobile node are referred to as "correspondent nodes". Mobile nodes can provide information about their current location to correspondent nodes, again using Binding Updates and Acknowledgements. Additionally, return routability test is performed between the mobile node, home agent, and the correspondent node in order to authorize the establishment of the binding. Packets between the mobile node and the correspondent node are either tunneled via the home agent, or sent directly if a binding exists in the correspondent node for the current location of the mobile node.

Mobile IPv6 tunnels payload packets between the mobile node and the home agent in both directions. This tunneling uses IPv6 encapsulation [6]. Where these tunnels need to be secured, they are replaced by IPsec tunnels [2].

Mobile IPv6 also provides support for the reconfiguration of the home network. Here, the home subnet prefixes may change over time. Mobile nodes can learn new information about home subnet prefixes through the "prefix discovery" mechanism.

This document discusses security mechanisms for the control traffic between the mobile node and the home agent. If this traffic is not protected, mobile nodes and correspondent nodes are vulnerable to man-in-the-middle, hijacking, passive wiretapping, impersonation, and denial-of-service attacks. Any third parties are also vulnerable to denial-of-service attacks, for instance if an attacker could direct the traffic flowing through the home agent to a innocent third party. These attacks are discussed in more detail in Section 15.1 of the Mobile IPv6 base specification [7].

In order to avoid these attacks, the base specification uses IPsec Encapsulating Security Payload (ESP) [3] to protect control traffic between the home agent and the mobile node. This control traffic consists of various messages carried by the Mobility Header protocol in IPv6 [5]. The traffic takes the following forms:

- Binding Update and Acknowledgement messages exchanged between the mobile node and the home agent, as described in Sections 10.3.1, 10.3.2, 11.7.1, and 11.7.3 of the base specification [7].

- Return routability messages Home Test Init and Home Test that pass through the home agent on their way to a correspondent node, as described in Section 10.4.6 of the base specification [7].

- ICMPv6 messages exchanged between the mobile node and the home agent for the purposes of prefix discovery, as described in Sections 10.6 and 11.4 of the base specification [7].

The nodes may also optionally protect payload traffic passing through the home agent, as described in Section 5.5 of the base specification [7]. If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection support is required.

The control traffic between the mobile node and the home agent requires message authentication, integrity, correct ordering and anti-replay protection. The mobile node and the home agent must have an IPsec security association to protect this traffic. IPsec does not proving correct ordering of messages. Correct ordering of the control traffic is ensured by a sequence number in the Binding Update and Binding Acknowledgement messages. The sequence number in the Binding Updates also provides protection to a certain extent. It fails in some scenarios, for example, if the Home Agent loses the Binding Cache state. Full protection against replay attacks is possible only when IKE is used.

Great care is needed when using IKE [4] to establish security associations to Mobile IPv6 home agents. The right kind of addresses must be used for transporting IKE. This is necessary to avoid circular dependencies in which the use of a Binding Update triggers the need for an IKE exchange that cannot complete prior to the Binding Update having been completed.

The mobile IPv6 base document defines the main requirements the mobile nodes and home agents must follow when securing the above traffic. This document discusses these requirements in more depth, illustrates the used packet formats, describes suitable configuration procedures, and shows how implementations can process the packets in the right order.

We begin our description by showing the required wire formats for the protected packets in Section 3. Section 4 describes rules which associated Mobile IPv6, IPsec, and IKE implementations must observe. Section 5 discusses how to configure either manually keyed IPsec security associations or how to configure IKE to establish them automatically. Section 6 shows examples of how packets are processed within the nodes.

All implementations of Mobile IPv6 mobile node and home agent MUST support at least the formats described in Section 3 and obey the rules in Section 4.

The configuration and processing sections are informative, and should only be considered as one possible way of providing the required functionality.

Note that where this document indicates a feature MUST be supported and SHOULD be used, this implies that all implementations must be capable of using the specified feature, but there may be cases where, for instance, a configuration option disables to use of the feature in a particular situation.

2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

3. Packet Formats

3.1. Binding Updates and Acknowledgements

When the mobile node is away from its home, the BUs sent by it to the home agent MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header in transport mode
```

```
   Mobility header
      Binding Update
         Alternate Care-of Address option (care-of address)
```

Note that the Alternate Care-of Address option is used to ensure that the care-of address is protected by ESP. The home agent considers the address within this option as the current care-of address for the mobile node. The home address is not protected by ESP directly, but the use of a specific home address with a specific security association is required by policy.

The Binding Acknowledgements sent back to the mobile node when it is away from home MUST support at least the following headers in the following order:

```
   IPv6 header (source = home agent,
                destination = care-of address)
   Routing header (type 2)
      home address
   ESP header in transport mode
   Mobility header
      Binding Acknowledgement
```

When the mobile node is at home, the above rules are different as the mobile node can use its home address as a source address. This typically happens for the de-registration Binding Update when the mobile is returning home. In this situation, the Binding Updates MUST support at least the following headers in the following order:

```
   IPv6 header (source = home address,
                destination = home agent)
   ESP header in transport mode
   Mobility header
      Binding Update
```

The Binding Acknowledgement messages sent to the home address MUST support at least the following headers in the following order:

```
   IPv6 header (source = home agent,
                destination = home address)
   ESP header in transport mode
   Mobility header
      Binding Acknowledgement
```

3.2. Return Routability Signaling

When the Home Test Init messages tunneled to the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Mobility Header
   Home Test Init
```

This format assumes that the mobile node's current care-of address is used as the outer header destination address in the security association. As discussed in Section 4.3, this requires the home agent to update the destination address when the mobile node moves. Policy entries and security association selectors stay the same, however, as the inner packets do not change upon movements.

Note that there are trade-offs in using care-of addresses as the destination addresses versus using the home address and attaching an additional Home Address destination option and/or Routing header to the packets. The basis for requiring support for at least the care-of address case has been discussed in Section 7.

Similarly, when the Home Test messages tunneled from the home agent are protected by IPsec, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header in tunnel mode
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test
```

The format used to protect return routability packets relies on the destination of the tunnel packets to change for the mobile node as it moves. The home agent's address stays the same, but the mobile node's address changes upon movements, as if the security association's outer header destination address had changed. When the mobile node adopts a new care-of address, it adopts also a new source address for outgoing tunnel packets. The home agent accepts packets sent like this, as the outer source address in tunnel packets is not checked according to the rules in RFC 2401. (We note, however, that some implementations are known to make source address checks.) For a discussion of the role of source addresses in outer tunnel headers, see Section 5.1.2.1 of RFC 2401 [2]. Note also that the home agent requires the packets to be authenticated regardless of the source address change, hence the "new" sender must possess the same keys for the security association as it had in the previous location. This proves that the sender is the same entity, regardless of the changes in the addresses.

The process is more complicated in the home agent side, as the home agent has stored the previous care-of address in its Security Association Database as the outer header destination address. When IKE is being used, the mobile node runs it on top of its current care-of address, and the resulting tunnel-mode security associations will use the same addresses as IKE run over. In order for the home agent to be able to tunnel a Home Test message to the mobile node, it uses the current care-of address as the destination of the tunnel packets, as if the home agent had modified the outer header destination address in the security association used for this protection. This implies that the same security association can be used in multiple locations, and no new configuration or re-establishment of IKE phases is needed per movement. Section 5.2.2 discusses the security policy and security association database entries that are needed to accomplish this.

3.3. Prefix Discovery

If IPsec is used to protect prefix discovery, requests for prefixes from the mobile node to the home agent MUST support at least the following headers in the following order.

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header in transport mode
ICMPv6
   Mobile Prefix Solicitation
```

Again if IPsec is used, solicited and unsolicited prefix information advertisements from the home agent to the mobile node MUST support at least the following headers in the following order.

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header in transport mode
```

```
ICMPv6
   Mobile Prefix Advertisement
```

3.4. Payload Packets

If IPsec is used to protect payload packets tunneled to the home agent from the mobile node, we use a format similar to the one in Section 3.2. However, instead of the MobilityHeader, these packets may contain any legal IPv6 protocol(s):

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header in tunnel mode
IPv6 header (source = home address,
             destination = correspondent node)
Any protocol
```

Similarly, when the payload packets are tunneled from the home agent to the mobile node with ESP encapsulation, they MUST support at least the following headers in the following order:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header in tunnel mode
IPv6 header (source = correspondent node,
             destination = home address)
Any protocol
```

4. Requirements

This section describes mandatory rules for all Mobile IPv6 mobile nodes and home agents. These rules are necessary in order for it to be possible to enable IPsec communications despite movements, guarantee sufficient security, and to ensure correct processing order of packets.

The rules in the following sections apply only to the communications between home agents and mobile nodes. They should not be taken as requirements on how IPsec in general is used by mobile nodes.

4.1. Mandatory Support

The following requirements apply to both home agents and mobile nodes:

- o Manual configuration of IPsec security associations MUST be supported. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent.

- o Automatic key management with IKE [4] MAY be supported. Only IKEv1 is discussed in this document. Other automatic key management mechanisms exist and will appear beyond IKEv1, but this document does not address the issues related to them.

- o ESP encapsulation of Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- o ESP encapsulation of the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- o ESP encapsulation of the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- o ESP encapsulation of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- o If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported for those protocols.

4.2. Policy Requirements

The following requirements apply to both home agents and mobile nodes:

- o As required in the base specification [7], when a packet destined to the receiving node is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option is considered as the source address of the packet.

  Note that the home address option appears before IPsec headers. Section 11.3.2 of the base specification describes one possible implementation approach for this: The IPsec policy operations can be performed at the time when the packet has not yet been modified per Mobile IPv6 rules, or has been brought back to its normal form after Mobile IPv6 processing. That is, the processing of the Home Address option is seen as a fixed transformation of the packets that does not affect IPsec processing.

- Similarly, a home address within a Type 2 Routing header destined to the receiving node is considered as the destination address of the packet, when a packet is matched against IPsec security policy or selectors of a security association.

  Similar implementation considers apply to the Routing header processing as was described above for the Home Address destination option.

- When IPsec is used to protect return routability signaling or payload packets, this protection MUST only be applied to the return routability packets entering the IPv6 encapsulated tunnel interface between the mobile node and the home agent. This can be achieved, for instance, by defining the security policy database entries specifically for the tunnel interface. That is, the policy entries are not generally applied on all traffic on the physical interface(s) of the nodes, but rather only on traffic that enters this tunnel.

- The authentication of mobile nodes MAY be based either on machine or user credentials. Note that multi-user operating systems typically allow all users of a node to use any of the IP addresses assigned to the node. This limits the capability of the home agent to restrict the use of a home address to a particular user in such environment. Where user credentials are applied in a multi-user environment, the configuration should authorize all users of the node to control all home addresses assigned to the node.

- When the mobile node returns home and de-registers with the Home Agent, the tunnel between the home agent and the mobile node's care-of address is torn down. The security policy entries, which were used for protecting tunneled traffic between the mobile node and the home agent MUST be made inactive (for instance, by removing them and installing them back later through an API). The corresponding security associations could be kept as they are or deleted depending on how they were created. If the security associations were created dynamically using IKE, they are automatically deleted when they expire. If the security associations were created through manual configuration, they MUST be retained and used later when the mobile node moves away from home again. The security associations protecting Binding Updates and Acknowledgements, and prefix discovery SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

The following rules apply to mobile nodes:

- o The mobile node MUST use the Home Address destination option in Binding Updates and Mobile Prefix Solicitations, sent to the home agent from a care-of address.

- o When the mobile node receives a changed set of prefixes from the home agent during prefix discovery, there is a need to configure new security policy entries, and there may be a need to configure new security associations. It is outside the scope of this specification to discuss automatic methods for this.

The following rules apply to home agents:

- o The home agent MUST use the Type 2 Routing header in Binding Acknowledgements and Mobile Prefix Advertisements sent to the mobile node, again due to the need to have the home address visible when the policy checks are made.

- o It is necessary to avoid the possibility that a mobile node could use its security association to send a Binding Update on behalf of another mobile node using the same home agent. In order to do this, the security policy database entries MUST unequivocally identify a single security association for protecting Binding Updates between any given home address and home agent when manually keyed IPsec security associations are used. When dynamic keying is used, the security policy database entries MUST unequivocally identify the IKE phase 1 credentials which can be used to authorize the creation of security associations for protecting Binding Updates for a particular home address. How these mappings are maintained is outside the scope of this specification, but they may be maintained, for instance, as a locally administered table in the home agent. If the phase 1 identity is a Fully Qualified Domain Name (FQDN), secure forms of DNS may also be used.

- o When the set of prefixes advertised by the home agent changes, there is a need to configure new security policy entries, and there may be a need to configure new security associations. It is outside the scope of this specification to discuss automatic methods for this, if new home addresses are required.

4.3. IPsec Protocol Processing

The following requirements apply to both home agents and mobile nodes:

o When securing Binding Updates, Binding Acknowledgements, and prefix discovery, both the mobile nodes and the home agents MUST support and SHOULD use the Encapsulating Security Payload (ESP) [3] header in transport mode and MUST use a non-null payload authentication algorithm to provide data origin authentication, connectionless integrity and optional anti-replay protection.

  Mandatory support for encryption and integrity protection algorithms is as defined in RFC 2401 [2], RFC 2402 [8], and RFC 2406 [3]. Care is needed when selecting suitable encryption algorithms for ESP, however. Currently available integrity protection algorithms are in general considered to be secure. The encryption algorithm, DES, mandated by the current IPsec standards is not, however. This is particularly problematic when IPsec security associations are configured manually, as the same key is used for a long time.

o Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure. A non-null encryption transform and a non-null authentication algorithm MUST be applied.

  Note that the return routability procedure involves two message exchanges from the mobile node to the correspondent node. The purpose of these exchanges is to assure that the mobile node is live at the claimed home and care-of addresses. One of the exchanges is sent directly to and from the correspondent node, while another one is tunneled through the home agent. If an attacker is on the mobile node's link and the mobile node's current link is an unprotected wireless link, the attacker would able to see both sets of messages, and launch attacks based on it (these attacks are discussed further in Section 15.4 of the base specification [7].) One can prevent the attack by making sure that the packets tunneled through the home agent are encrypted.

  Note that this specification concerns itself only with on-the-wire formats, and does not dictate specific implementations mechanisms. In the case of IPsec tunnel mode, the use of IP-in-IP encapsulation followed by IPsec transport mode encapsulation may also be possible.

The following rules apply to mobile nodes:

- o When ESP is used to protect Binding Updates, there is no protection for the care-of address which appears in the IPv6 header outside the area protected by ESP. It is important for the home agent to verify that the care-of address has not been tampered with. As a result, the attacker would have redirected the mobile node's traffic to another address. In order to prevent this, Mobile IPv6 implementations MUST use the Alternate Care-of Address mobility option in Binding Updates sent by mobile nodes while away from home. The exception to this is when the mobile node returns home and sends a Binding Update to the home agent in order to de-register. In this case no Alternate Care-of Address option is needed, as described in Section 3.1.

  When IPsec is used to protect return routability signaling or payload packets, the mobile node MUST set the source address it uses for the outgoing tunnel packets to the current primary care-of address. The mobile node starts to use a new primary care-of address immediately after sending a Binding Update to the home agent to register this new address. Similarly, it starts to use the new address as the required destination address of tunneled packets received from the home agent.

The following rules apply to home agents:

- o When IPsec is used to protect return routability signaling or payload packets, IPsec security associations are needed to provide this protection. When the care-of address for the mobile node changes as a result of an accepted Binding Update, special treatment is needed for the next packets sent using these security associations. The home agent MUST set the new care-of address as the destination address of these packets, as if the outer header destination address in the security association had changed. Similarly, the home agent starts to expect the new source address in the tunnel packets received from the mobile node.

  Such address changes can be implemented, for instance, through an API from the Mobile IPv6 implementation to the IPsec implementation. It should be noted that the use of such an API and the address changes MUST only be done based on the Binding Updates received by the home agent and protected by the use of IPsec. Address modifications based on other sources, such as Binding Updates to the correspondent nodes protected by return routability, or open access to an API from any application may result in security vulnerabilities.

4.4. Dynamic Keying

The following requirements apply to both home agents and mobile nodes:

- o If anti-replay protection is required, dynamic keying MUST be used. IPsec can provide anti-replay protection only if dynamic keying is used (which may not always be the case). IPsec also does not guarantee correct ordering of packets, only that they have not been replayed. Because of this, sequence numbers within the Mobile IPv6 messages are used to ensure correct ordering. However, if the 16 bit Mobile IPv6 sequence number space is cycled through, or the home agent reboots and loses its state regarding the sequence numbers, replay and reordering attacks become possible. The use of dynamic keying, IPsec anti-replay protection, and the Mobile IPv6 sequence numbers can together prevent such attacks.

- o If IKE version 1 is used with preshared secrets in main mode, it determines the shared secret to use from the IP address of the peer. With Mobile IPv6, however, this may be a care-of address and does not indicate which mobile node attempts to contact the home agent. Therefore, if preshared secret authentication is used in IKEv1 between the mobile node and the home agent then aggressive mode MUST be used. Note also that care needs to be taken with phase 1 identity selection. Where the ID_IPV6_ADDR Identity Payloads is used, unambiguous mapping of identities to keys is not possible. (The next version of IKE may not have these limitations.)

Note that the difficulties with main mode and preshared secrets in IKE version 1 are well known for dynamic addresses. With static addresses, there has not been a problem. With Mobile IPv6, however, the use of the care-of addresses to run IKE to the home agent presents a problem even when the home address stays stable. Further discussion about the use of care-of addresses in this way appears in Section 7.

The following rules apply to mobile nodes:

- o In addition to the rules above, if dynamic keying is used, the key management protocol MUST use the care-of address as the source address in the protocol exchanges with the mobile node's home agent.

- However, the IPsec security associations with the mobile node's home agent use home addresses. That is, the IPsec security associations MUST be requested from the key management protocol using the home address of the mobile node as the client identity.

  The security associations for protecting Binding Updates and Acknowledgements are requested for the Mobility header protocol in transport mode and for specific IP addresses as endpoints. No other selectors are used. Similarly, the security associations for protecting prefix discovery are requested for the ICMPv6 protocol and the specific IP addresses, again without other selectors. Security associations for payload and return routability protection are requested for a specific tunnel interface and either the payload protocol or the Mobility header protocol, in tunnel mode. In this case one requested endpoint is an IP address and the other one is a wildcard, and there are no other selectors.

- If the mobile node has used IKE version 1 to establish security associations with its home agent, it should follow the procedures discussed in Section 11.7.1 and 11.7.3 of the base specification [7] to determine whether the IKE endpoints can be moved or if IKE phase 1 has to be re-established.

The following rules apply to home agents:

- If the home agent has used IKE version 1 to establish security associations with the mobile node, it should follow the procedures discussed in Section 10.3.1 and 10.3.2 of the base specification [7] to determine whether the IKE endpoints can be moved or if IKE phase 1 has to be re-established.

5. Example Configurations

In the following we describe the Security Policy Database (SPD) and Security Association Database (SAD) entries necessary to protect Binding Updates and Binding Acknowledgements exchanged between the mobile node and the home agent.

Section 5.1 introduces the format we use in the description of the SPD and the SAD. Section 5.2 describes how to configure manually keyed IPsec security associations without dynamic keying, and Section 5.3 describes how to use dynamic keying.

5.1. Format

The format used in the examples is as follows. The SPD description has the format

```
<node> "SPD OUT:"
  "-" <spdentry>
  "-" <spdentry>
  ...
  "-" <spdentry>

<node> "SPD IN:"
  "-" <spdentry>
  "-" <spdentry>
  ...
  "-" <spdentry>
```

Where <node> represents the name of the node, and <spdentry> has the following format:

```
"IF" <condition> "THEN USE SA " <sa> |
"IF" <condition> "THEN USE SA " <pattern> |
```

Where <condition> is a boolean expression about the fields of the IPv6 packet, <sa> is the name of a specific security association, and <pattern> is a specification for a security association to be negotiated via IKE [4]. The SAD description has the format

```
<node> "SAD:"
  "-" <sadentry>
  "-" <sadentry>
  ...
  "-" <sadentry>
```

Where <node> represents the name of the node, and <sadentry> has the following format:

```
<sa> "(" <dir> ","
         <spi> ","
         <destination> ","
         <ipsec-proto> ","
         <mode> ")" ":"
     <rule>
```

Where <dir> is "IN" or "OUT", <spi> is the SPI of the security association, <destination> is its destination, <ipsec-proto> is in our case "ESP", <mode> is either "TUNNEL" or "TRANSPORT", and <rule> is an expression which describes the IPsec selectors, i.e., which fields of the IPv6 packet must have which values.

We will be using an example mobile node in this section with the home address "home_address_1". The user's identity in this mobile node is "user_1". The home agent's address is "home_agent_1".

5.2. Manual Configuration

5.2.1. Binding Updates and Acknowledgements

Here are the contents of the SPD and SAD for protecting Binding Updates and Acknowledgements:

```
mobile node SPD OUT:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = MH
    THEN USE SA SA1

mobile node SPD IN:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = MH
    THEN USE SA SA2

mobile node SAD:
  - SA1(OUT, spi_a, home_agent_1, ESP, TRANSPORT):
    source = home_address_1 & destination = home_agent_1 &
    proto = MH
  - SA2(IN, spi_b, home_address_1, ESP, TRANSPORT):
    source = home_agent_1 & destination = home_address_1 &
    proto = MH

home agent SPD OUT:
  - IF source = home_agent_1 & destination = home_address_1 &
       proto = MH
    THEN USE SA SA2

home agent SPD IN:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = MH
    THEN USE SA SA1

home agent SAD:
  - SA2(OUT, spi_b, home_address_1, ESP, TRANSPORT):
    source = home_agent_1 & destination = home_address_1 &
```

```
        proto = MH
      - SA1(IN, spi_a, home_agent_1, ESP, TRANSPORT):
        source = home_address_1 & destination = home_agent_1 &
        proto = MH
```

In the above, "MH" refers to the protocol number for the Mobility Header [7].

5.2.2. Return Routability Signaling

In the following we describe the necessary SPD and SAD entries to protect return routability signaling between the mobile node and the home agent. Note that the rules in the SPD are ordered, and the ones in the previous section must take precedence over these ones. In other words, the higher precedence entries must occur first in the RFC 2401 [2] ordered list of SPD entries.

```
    mobile node SPD OUT:
      - IF interface = IPv6 IPv6 tunnel to home_agent_1 &
           source = home_address_1 & destination = any &
           proto = MH
        THEN USE SA SA3

    mobile node SPD IN:
      - IF interface = IPv6 tunnel from home_agent_1 &
           source = any & destination = home_address_1 &
           proto = MH
        THEN USE SA SA4

    mobile node SAD:
      - SA3(OUT, spi_c, home_agent_1, ESP, TUNNEL):
        source = home_address_1 & destination = any & proto = MH
      - SA4(IN, spi_d, care_of_address_1, ESP, TUNNEL):
        source = any & destination = home_address_1 & proto = MH

    home agent SPD OUT:
      - IF interface = IPv6 tunnel to home_address_1 &
           source = any & destination = home_address_1 &
           proto = MH
        THEN USE SA SA4

    home agent SPD IN:
      - IF interface = IPv6 tunnel from home_address_1 &
           source = home_address_1 & destination = any &
           proto = MH
        THEN USE SA SA3
```

```
      home agent SAD:
        - SA4(OUT, spi_d, care_of_address_1, ESP, TUNNEL):
          source = any & destination = home_address_1 & proto = MH
        - SA3(IN, spi_c, home_agent_1, ESP, TUNNEL):
          source = home_address_1 & destination = any & proto = MH
```

The security association from the home agent to the mobile node uses the current care-of address as the destination. As discussed earlier, this address is updated in the SAD as the mobile node moves. It can be initialized to the home address before the mobile node has registered.

5.2.3. Prefix Discovery

In the following we describe some additional SPD and SAD entries to protect prefix discovery. Note that the SPDs described above protect all ICMPv6 traffic between the mobile node and the home agent, as IPsec may not have the ability to distinguish between different ICMPv6 types.

```
      mobile node SPD OUT:
        - IF source = home_address_1 & destination = home_agent_1 &
             proto = ICMPv6
          THEN USE SA SA5.

      mobile node SPD IN:
        - IF source = home_agent_1 & destination = home_address_1 &
             proto = ICMPv6
          THEN USE SA SA6

      mobile node SAD:
        - SA5(OUT, spi_e, home_agent_1, ESP, TRANSPORT):
          source = home_address_1 & destination = home_agent_1 &
          proto = ICMPv6
        - SA6(IN, spi_f, home_address_1, ESP, TRANSPORT):
          source = home_agent_1 & destination = home_address_1 &
          proto = ICMPv6

      home agent SPD OUT:
        - IF source = home_agent_1 & destination = home_address_1 &
             proto = ICMPv6
          THEN USE SA SA6

      home agent SPD IN:
        - IF source = home_address_1 & destination = home_agent_1 &
             proto = ICMPv6
          THEN USE SA SA5
```

```
   home agent SAD:
     - SA6(OUT, spi_f, home_address_1, ESP, TRANSPORT):
       source = home_agent_1 & destination = home_address_1 &
       proto = ICMPv6
     - SA5(IN, spi_e, home_agent_1, ESP, TRANSPORT):
       source = home_address_1 & destination = home_agent_1 &
       proto = ICMPv6
```

5.2.4. Payload Packets

It is also possible to perform some additional, optional, protection of tunneled payload packets. This protection takes place in a similar manner to the return routability protection above, but requires a different value for the protocol field. The necessary SPD and SAD entries are shown below. It is assumed that the entries for protecting Binding Updates and Acknowledgements, and the entries to protect Home Test Init and Home Test messages take precedence over these entries.

```
   mobile node SPD OUT:
     - IF interface = IPv6 tunnel to home_agent_1 &
          source = home_address_1 & destination = any &
          proto = X
       THEN USE SA SA7

   mobile node SPD IN:
     - IF interface = IPv6 tunnel from home_agent_1 &
          source = any & destination = home_address_1 &
          proto = X
       THEN USE SA SA8

   mobile node SAD:
     - SA7(OUT, spi_g, home_agent_1, ESP, TUNNEL):
       source = home_address_1 & destination = any & proto = X
     - SA8(IN, spi_h, care_of_address_1, ESP, TUNNEL):
       source = any & destination = home_address_1 & proto = X

   home agent SPD OUT:
     - IF interface = IPv6 tunnel to home_address_1 &
          source = any & destination = home_address_1 &
          proto = X
       THEN USE SA SA8

   home agent SPD IN:
     - IF interface = IPv6 tunnel from home_address_1 &
          source = home_address_1 & destination = any &
          proto = X
       THEN USE SA SA7
```

```
   home agent SAD:
     - SA8(OUT, spi_h, care_of_address_1, ESP, TUNNEL):
       source = any & destination = home_address_1 & proto = X
     - SA7(IN, spi_g, home_agent_1, ESP, TUNNEL):
       source = home_address_1 & destination = any & proto = X
```

If multicast group membership control protocols such as MLDv1 [9] or MLDv2 [11] need to be protected, these packets may use a link-local address rather than the home address of the mobile node. In this case the source and destination can be left as a wildcard and the SPD entries will work solely based on the used interface and the protocol, which is ICMPv6 for both MLDv1 and MLDv2.

Similar problems are encountered when stateful address autoconfiguration protocols such as DHCPv6 [10] are used. The same approach is applicable for DHCPv6 as well. DHCPv6 uses the UDP protocol.

Support for multiple layers of encapsulation (such as ESP encapsulated in ESP) is not required by RFC 2401 [2] and is also otherwise often problematic. It is therefore useful to avoid setting the protocol X in the above entries to either AH or ESP.

5.3. Dynamic Keying

In this section we show an example configuration that uses IKE to negotiate security associations.

5.3.1. Binding Updates and Acknowledgements

Here are the contents of the SPD for protecting Binding Updates and Acknowledgements:

```
   mobile node SPD OUT:
     - IF source = home_address_1 & destination = home_agent_1 &
          proto = MH
       THEN USE SA ESP TRANSPORT: local phase 1 identity = user_1

   mobile node SPD IN:
     - IF source = home_agent_1 & destination = home_address_1 &
          proto = MH
       THEN USE SA ESP TRANSPORT: local phase 1 identity = user_1

   home agent SPD OUT:
     - IF source = home_agent_1 & destination = home_address_1 &
          proto = MH
       THEN USE SA ESP TRANSPORT: peer phase 1 identity = user_1
```

```
home agent SPD IN:
  - IF source = home_address_1 & destination = home_agent_1 &
       proto = MH
    THEN USE SA ESP TRANSPORT: peer phase 1 identity = user_1
```

We have omitted details of the proposed transforms in the above, and all details related to the particular authentication method such as certificates beyond listing a specific identity that must be used.

We require IKE version 1 to be run using the care-of addresses but still negotiate IPsec SAs that use home addresses. The extra conditions set by the home agent SPD for the peer phase 1 identity to be "user_1" must be verified by the home agent. The purpose of the condition is to ensure that the IKE phase 2 negotiation for a given user's home address can not be requested by another user. In the mobile node, we simply set our local identity to be "user_1".

These checks also imply that the configuration of the home agent is user-specific: every user or home address requires a specific configuration entry. It would be possible to alleviate the configuration tasks by using certificates that have home addresses in the Subject AltName field. However, it is not clear if all IKE implementations allow one address to be used for carrying the IKE negotiations when another address is mentioned in the used certificates. In any case, even this approach would have required user-specific tasks in the certification authority.

5.3.2. Return Routability Signaling

Protection for the return routability signaling can be configured in a similar manner as above.

```
mobile node SPD OUT:
  - IF interface = IPv6 tunnel to home_agent_1 &
       source = home_address_1 & destination = any &
       proto = MH
    THEN USE SA ESP TUNNEL: outer destination = home_agent_1 &
                            local phase 1 identity = user_1

mobile node SPD IN:
  - IF interface = IPv6 tunnel from home_agent_1 &
       source = any & destination = home_address_1 &
       proto = MH
    THEN USE SA ESP TUNNEL: outer destination = home_agent_1 &
                            local phase 1 identity = user_1
```

```
   home agent SPD OUT:
     - IF interface = IPv6 tunnel to home_address_1 &
          source = any & destination = home_address_1 &
          proto = MH
       THEN USE SA ESP TUNNEL: outer destination = home_address_1 &
                               peer phase 1 identity = user_1

   home agent SPD IN:
     - IF interface = IPv6 tunnel from home_address_1 &
          source = home_address_1 & destination = any &
          proto = MH
       THEN USE SA ESP TUNNEL: outer destination = home_address_1 &
                               peer phase 1 identity = user_1
```

The security association from the home agent to the mobile node uses the current care-of address as the destination. As discussed earlier, this address is updated in the SAD as the mobile node moves. The SPD entries can be written using the home address (as above), if the care-of address update in the SAD is also done upon the creation of security associations.

5.3.3. Prefix Discovery

In the following we describe some additional SPD entries to protect prefix discovery with IKE. (Note that when actual new prefixes are discovered, there may be a need to enter new manually configured SPD entries to specify the authorization policy for the resulting new home addresses.)

```
   mobile node SPD OUT:
     - IF source = home_address_1 & destination = home_agent_1 &
          proto = ICMPv6
       THEN USE SA ESP TRANSPORT: local phase 1 identity = user_1

   mobile node SPD IN:
     - IF source = home_agent_1 & destination = home_address_1 &
          proto = ICMPv6
       THEN USE SA ESP TRANSPORT: local phase 1 identity = user_1

   home agent SPD OUT:
     - IF source = home_agent_1 & destination = home_address_1 &
          proto = ICMPv6
       THEN USE SA ESP TRANSPORT: peer phase 1 identity = user_1

   home agent SPD IN:
     - IF source = home_address_1 & destination = home_agent_1 &
          proto = ICMPv6
       THEN USE SA ESP TRANSPORT: peer phase 1 identity = user_1
```

5.3.4. Payload Packets

Protection for the payload packets happens similarly to the protection of return routability signaling. As in the manually keyed case, these SPD entries have lower priority than the above ones.

```
   mobile node SPD OUT:
     - IF interface = IPv6 tunnel to home_agent_1 &
          source = home_address_1 & destination = any &
          proto = X
       THEN USE SA ESP TUNNEL: outer destination = home_agent_1 &
                               local phase 1 identity = user_1

   mobile node SPD IN:
     - IF interface = IPv6 tunnel from home_agent_1 &
          source = any & destination = home_address_1 &
          proto = X
       THEN USE SA ESP TUNNEL: outer destination = home_agent_1 &
                               local phase 1 identity = user_1

   home agent SPD OUT:
     - IF interface = IPv6 tunnel to home_address_1 &
          source = any & destination = home_address_1 &
          proto = X
       THEN USE SA ESP TUNNEL: outer destination = home_address_1 &
                               peer phase 1 identity = user_1

   home agent SPD IN:
     - IF interface = IPv6 tunnel from home_address_1 &
          source = home_address_1 & destination = any &
          proto = X
       THEN USE SA ESP TUNNEL: outer destination = home_address_1 &
                               peer phase 1 identity = user_1
```

6. Processing Steps within a Node

6.1. Binding Update to the Home Agent

Step 1. At the mobile node, Mobile IPv6 module first produces the following packet:

```
   IPv6 header (source = home address,
                destination = home agent)
   Mobility header
      Binding Update
```

Step 2. This packet is matched against the IPsec SPD on the mobile node and we make a note that IPsec must be applied.

Step 3. Then, we add the necessary Mobile IPv6 options but do not change the addresses yet, as described in Section 11.3.2 of the base specification [7]. This results in:

```
IPv6 header (source = home address,
             destination = home agent)
Destination Options header
   Home Address option (care-of address)
Mobility header
   Binding Update
```

Step 4. Finally, IPsec headers are added and the necessary authenticator values are calculated:

```
IPv6 header (source = home address,
             destination = home agent)
Destination Options header
   Home Address option (care-of address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

Here spi_a is the SPI value that was either configured manually, or agreed upon in an earlier IKE negotiation.

Step 5. Before sending the packet, the addresses in the IPv6 header and the Destination Options header are changed:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

6.2. Binding Update from the Mobile Node

Step 1. The following packet is received at the home agent:

```
IPv6 header (source = care-of address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

Step 2. The home address option is processed first, which results in

```
IPv6 header (source = home address,
             destination = home agent)
Destination Options header
   Home Address option (care-of address)
ESP header (SPI = spi_a)
Mobility header
   Binding Update
```

Step 3. ESP header is processed next, resulting in

```
IPv6 header (source = home address,
             destination = home agent)
Destination Options header
   Home Address option (care-of address)
Mobility header
   Binding Update
```

Step 4. This packet matches the policy required for this security association (source = home address, destination = home agent, proto = MH).

Step 5. Mobile IPv6 processes the Binding Update. The Binding Update is delivered to the Mobile IPv6 module.

Step 6. If there are any security associations in the security association database for the protection of return routability or payload packets for this mobile node, those security associations are updated with the new care-of address.

6.3. Binding Acknowledgement to the Mobile Node

Step 1. Mobile IPv6 produces the following packet:

```
IPv6 header (source = home agent,
             destination = home address)
Mobility header
   Binding Acknowledgement
```

Step 2. This packet matches the IPsec policy entries, and we remember that IPsec has to be applied.

Step 3. Then, we add the necessary Route Headers but do not change the addresses yet, as described in Section 9.5.4 of the base specification [7]. This results in:

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
Mobility header
   Binding Acknowledgement
```

Step 4. We apply IPsec:

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

Step 5. Finally, before sending the packet out we change the addresses in the IPv6 header and the Route header:

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

6.4. Binding Acknowledgement from the Home Agent

Step 1. The following packet is received at the mobile node

```
IPv6 header (source = home agent,
             destination = care-of address)
Routing header (type 2)
   home address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

Step 2. After the routing header is processed the packet becomes

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
ESP header (SPI = spi_b)
Mobility header
   Binding Acknowledgement
```

Step 3. ESP header is processed next, resulting in:

```
IPv6 header (source = home agent,
             destination = home address)
Routing header (type 2)
   care-of address
Mobility header
   Binding Acknowledgement
```

Step 4. This packet matches the policy required for this security association (source = home agent, destination = home address, proto = MH).

Step 5. The Binding Acknowledgement is delivered to the Mobile IPv6 module.

6.5. Home Test Init to the Home Agent

Step 1. The mobile node constructs a Home Test Init message:

```
IPv6 header (source = home address,
             destination = correspondent node)
Mobility header
   Home Test Init
```

Step 2. Mobile IPv6 determines that this packet should go to the tunnel to the home agent.

Step 3. The packet is matched against IPsec policy entries for the interface, and we find that IPsec needs to be applied.

Step 4. IPsec tunnel mode headers are added. Note that we use a care-of address as a source address for the tunnel packet.

```
IPv6 header (source = care-of address,
             destination = home agent)
ESP header (SPI = spi_c)
IPv6 header (source = home address,
```

```
                 destination = correspondent node)
   Mobility header
      Home Test Init
```

Step 5. The packet is sent directly to the home agent using IPsec encapsulation.

6.6. Home Test Init from the Mobile Node

Step 1. The home agent receives the following packet:

```
   IPv6 header (source = care-of address,
                destination = home agent)
   ESP header (SPI = spi_c)
   IPv6 header (source = home address,
                destination = correspondent node)
   Mobility Header
      Home Test Init
```

Step 2. IPsec processing is performed, resulting in:

```
   IPv6 header (source = home address,
                destination = correspondent node)
   Mobility Header
      Home Test Init
```

Step 3. The resulting packet matches the policy required for this security association and the packet can be processed further.

Step 4. The packet is then forwarded to the correspondent node.

6.7. Home Test to the Mobile Node

Step 1. The home agent receives a Home Test packet from the correspondent node:

```
   IPv6 header (source = correspondent node,
                destination = home address)
   Mobility Header
      Home Test Init
```

Step 2. The home agent determines that this packet is destined to a mobile node that is away from home, and decides to tunnel it.

Step 3. The packet matches the IPsec policy entries for the tunnel interface, and we note that IPsec needs to be applied.

Step 4. IPsec is applied, resulting in a new packet. Note that the home agent must keep track of the location of the mobile node, and update the tunnel endpoint address in the security association(s) accordingly.

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header (SPI = spi_d)
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test Init
```

Step 5. The packet is sent directly to the care-of address using IPsec encapsulation.

6.8. Home Test from the Home Agent

Step 1. The mobile node receives the following packet:

```
IPv6 header (source = home agent,
             destination = care-of address)
ESP header (SPI = spi_d)
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test Init
```

Step 2. IPsec is processed, resulting in:

```
IPv6 header (source = correspondent node,
             destination = home address)
Mobility Header
   Home Test Init
```

Step 3. This matches the policy required for this security association (source = any, destination = home address).

Step 4. The packet is given to Mobile IPv6 processing.

6.9. Prefix Solicitation Message to the Home Agent

This procedure is similar to the one presented in Section 6.1.

6.10. Prefix Solicitation Message from the Mobile Node

This procedure is similar to the one presented in Section 6.2.

6.11. Prefix Advertisement Message to the Mobile Node

This procedure is similar to the one presented in Section 6.3.

6.12. Prefix Advertisement Message from the Home Agent

This procedure is similar to the one presented in Section 6.4.

6.13. Payload Packet to the Home Agent

This procedure is similar to the one presented in Section 6.5.

6.14. Payload Packet from the Mobile Node

This procedure is similar to the one presented in Section 6.6.

6.15. Payload Packet to the Mobile Node

This procedure is similar to the one presented in Section 6.7.

6.16. Payload Packet from the Home Agent

This procedure is similar to the one presented in Section 6.8.

6.17. Establishing New Security Associations

Step 1. The mobile node wishes to send a Binding Update to the home agent.

```
IPv6 header (source = home address,
             destination = home agent)
Mobility header
   Binding Update
```

Step 2. There is no existing security association to protect the Binding Update, so the mobile node initiates IKE. The IKE packets are sent as shown in the following examples. The first packet is an example of an IKE packet sent from the mobile node, and the second one is from the home agent. The examples shows also that the phase 1 identity used for the mobile node is a FQDN.

```
IPv6 header (source = care-of address,
             destination = home agent)
   UDP
   IKE
      ... IDii = ID_FQDN mn123.ha.net ...
```

```
IPv6 header (source = home agent
             destination = care-of address)
   UDP
   IKE
      ... IDir = ID_FQDN ha.net ...
```

Step 3. IKE phase 1 completes, and phase 2 is initiated to request security associations for protecting traffic between the mobile node's home address and the home agent. These addresses will be used as selectors. This involves sending and receiving additional IKE packets. The below example shows again one packet sent by the mobile node and another sent by the home agent. The example shows also that the phase 2 identity used for the mobile node is the mobile node's home address.

```
IPv6 header (source = care-of address,
             destination = home agent)
   UDP
   IKE
      ... IDci = ID_IPV6_ADDR home address ...

IPv6 header (source = home agent,
             destination = care-of address)
   UDP
   IKE
      ... IDcr = ID_IPV6_ADDR home agent ...
```

Step 4. The remaining steps are as shown in Section 6.1.

6.18. Rekeying Security Associations

Step 1. The mobile node and the home agent have existing security associations. Either side may decide at any time that the security associations need to be rekeyed, for instance, because the specified lifetime is approaching.

Step 2. Mobility header packets sent during rekey may be protected by the existing security associations.

Step 3. When the rekeying is finished, new security associations are established. In practice there is a time interval during which an old, about-to-expire security association and newly established security association will both exist. The new ones should be used as soon as they become available.

Step 4. A notification of the deletion of the old security associations is received. After this, only the new security associations can be used.

Note that there is no requirement that the existence of the IPsec and IKE security associations is tied to the existence of bindings. It is not necessary to delete a security association if a binding is removed, as a new binding may soon be established after this.

Since cryptographic acceleration hardware may only be able to handle a limited number of active security associations, security associations may be deleted via IKE in order to keep the number of active cryptographic contexts to a minimum. Such deletions should not be interpreted as a sign of losing a contact to the peer or as a reason to remove a binding. Rather, if additional traffic needs to be sent, it is preferable to bring up another security association to protect it.

6.19. Movements and Dynamic Keying

In this section we describe the sequence of events that relate to movement with IKE-based security associations. In the initial state, the mobile node is not registered in any location and has no security associations with the home agent. Depending on whether the peers will be able to move IKE endpoints to new care-of addresses, the actions taken in Step 9 and 10 are different.

Step 1. Mobile node with the home address A moves to care-of address B.

Step 2. Mobile node runs IKE from care-of address B to the home agent, establishing a phase 1. The home agent can only act as the responder before it knows the current location of the mobile node.

Step 3. Protected by this phase 1, mobile node establishes a pair of security associations for protecting Mobility Header traffic to and from the home address A.

Step 4. Mobile node sends a Binding Update and receives a Binding Acknowledgement using the security associations created in Step 3.

Step 5. Mobile node establishes a pair of security associations for protecting return routability packets. These security associations are in tunnel mode and their endpoint in the mobile node side is care-of address B. For the purposes of our example, this step uses the phase 1 connection established in Step 2. Multiple phase 1 connections are also possible.

Step 6. The mobile node uses the security associations created in Step 5 to run return routability.

Step 7. The mobile node moves to a new location and adopts a new care-of address C.

Step 8. Mobile node sends a Binding Update and receives a Binding Acknowledgement using the security associations created in Step 3. The home agent ensures that the next packets sent using the security associations created in Step 5 will have the new care-of address as their destination address, as if the outer header destination address in the security association had changed.

Step 9. If the mobile node and the HA have the capability to change the IKE endpoints, they change the address to C. If they do not have the capability, both nodes remove their phase 1 connections created on top of the care-of address B and will establish a new IKE phase 1 on top of the care-of address C. This capability to change the IKE phase 1 end points is indicated through setting the Key Management Mobility Capability (K) flag [7] in the Binding Update and Binding Acknowledgement messages.

Step 10. If a new IKE phase 1 connection was setup after movement, the MN will not be able to receive any notifications delivered on top of the old IKE phase 1 security association. Notifications delivered on top of the new security association are received and processed normally. If the mobile node and HA were able to update the IKE endpoints, they can continue using the same IKE phase 1 connection.

7. Implementation Considerations

7.1. IPsec

Note that packet formats and header ordering discussed in Section 3 must be supported, but implementations may also support other formats. In general, the use of formats not required here may lead to incorrect processing of the packets by the peer (such as silently discarding them), unless support for these formats has been verified off-line. Such verification can take place at the same time the parameters of the security associations are agreed upon. In some cases, however, basic IPv6 specifications call for support of options not discussed here. In these cases, such a verification step might be unnecessary as long as the peer fully supports the relevant IPv6 specifications. However, no claims are made in this document about the validity of these other formats in the context of Mobile IPv6. It is also likely that systems that support Mobile IPv6 have been tested more extensively with the required formats.

We have chosen to require an encapsulation format for return routability and payload packet protection which can only be realized if the destination of the IPsec packets sent from the home agent can be changed as the mobile node moves. One of the main reasons for choosing such a format is that it removes the overhead of twenty four bytes when a home address option or routing header is added to the tunneled packet. Such an overhead would not be significant for the protection of the return routability packets, but would create an additional overhead if IPsec is used to protect the tunneling of payload packets to the home agent. This overhead may be significant for real-time traffic. Given that the use of the shorter packet formats for any traffic requires the existence of suitable APIs, we have chosen to require support for the shorter packet formats both for payload and return routability packets.

In order to support the care-of address as the destination address on the mobile node side, the home agent must act as if the outer header destination address in the security association to the mobile node would have changed upon movements. Implementations are free to choose any particular method to make this change, such as using an API to the IPsec implementation to change the parameters of the security association, removing the security association and installing a new one, or modification of the packet after it has gone through IPsec processing. The only requirement is that after registering a new binding at the home agent, the next IPsec packets sent on this security association will be addressed to the new care-of address.

We have chosen to require policy entries that are specific to a tunnel interface. This means that implementations have to regard the Home Agent - Mobile Node tunnel as a separate interface on which IPsec SPDs can be based. A further complication of the IPsec processing on a tunnel interface is that this requires access to the BITS implementation before the packet actually goes out.

7.2. IKE

We have chosen to require that a dynamic key management protocol must be able to make an authorization decision for IPsec security association creation with different addresses than with what the key management protocol is run. We expect this to be done typically by configuring the allowed combinations of phase 1 user identities and home addresses.

When certificate authentication is used, IKE fragmentation can be encountered. This can occur when certificate chains are used, or even with single certificates if they are large. Many firewalls do not handle fragments properly, and may drop them. Routers in the path may also discard fragments after the initial one, since they typically will not contain full IP headers that can be compared against an access list. Where fragmentation occurs, the endpoints will not always be able to establish a security association.

Fortunately, typical Mobile IPv6 deployment uses short certificate chains, as the mobile node is communicating directly with its home network. Where the problem appears, it may be difficult (at least away from home) to replace the firewalls or routers with equipment that can properly support fragments. It may help to store the peer certificates locally, or to obtain them through other means.

7.3. Bump-in-the-Stack

Mobile IPv6 sets high requirements for a so-called Bump-In-The-Stack (BITS) implementation model of IPsec. As Mobile IPv6 specific modifications of the packets are required before or after IPsec processing, the BITS implementation has to perform also some tasks related to mobility. This may increase the complexity of the implementation, even if it already performs some tasks of the IP layer (such as fragmentation).

Specifically, Bump-in-the-Stack implementations may have to deal with the following issues:

- o Processing the Home Address destination option and Routing header type 2 to a form suitable for IPsec processing to take place. This is needed, among other things, for the security association and policy lookups. While relatively straightforward, the required processing may have a hardware effect in BITS implementations, if they use hardware support beyond the cryptographic operations.

- o Detecting packets sent between the mobile node and its home agent using IPv6 encapsulation.

- o Offering the necessary APIs for updating the IPsec and IKE security association endpoints.

8. IANA Considerations

No IANA actions are necessary based on this document. IANA actions for the Mobile IPv6 protocol itself have been covered in [7].

9. Security Considerations

The Mobile IPv6 base specification [7] requires strong security between the mobile node and the home agent. This memo discusses how that security can be arranged in practice, using IPsec. The security considerations related to this are documented in the base specification, including a discussion of the implications of using either manual or dynamic keying.

10. References

10.1. Normative References

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

[2] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[3] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

[4] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[5] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[6] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

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

10.2. Informative References

[8] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.

[9] Deering, S., Fenner, W. and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[10] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[11] Vida, R. and L. Costa, Eds., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

11. Acknowledgements

The authors would like to thank Greg O'Shea, Michael Thomas, Kevin Miles, Cheryl Madson, Bernard Aboba, Erik Nordmark, Gabriel Montenegro, Steven Kent, and Santeri Paavolainen for interesting discussions in this problem space.

12. Authors' Addresses

Jari Arkko
Ericsson
02420 Jorvas
Finland

EMail: jari.arkko@ericsson.com

Vijay Devarapalli
Nokia Research Center
313 Fairchild Drive
Mountain View CA 94043
USA

EMail: vijayd@iprg.nokia.com

Francis Dupont
ENST Bretagne
Campus de Rennes
2, rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
France

EMail: Francis.Dupont@enst-bretagne.fr

13. Full Copyright Statement

Intellectual Property

Acknowledgement

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