Network Working Group
INTERNET-DRAFT
Category: Standards Track
<draft-ietf-mobileip-mipv6-ha-ipsec-01.txt>

Jari Arkko
Ericsson
Vijay Devarapalli
Nokia
Francis Dupont
ENST Bretagne

15 October 2002

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

1. Status of this Memo

The distribution of this memo is unlimited. It is filed as <draft-ietf-mobileip-mipv6-haipsec-00.txt>, and expires March 10, 2003. Please send comments to the author or to the Mobile IP working group mailing list.

2. 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 draft 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.

3. Contents

4. Introduction

Mobile IPv6 [1] uses IPsec [2] to protect signaling between the home agent and the mobile node. This signaling consists of various messages carried by the Mobility Header protocol in IPv6. This signaling traffic takes the following forms:

(1) Binding Update and Acknowledgement messages exchanged between the mobile node and the home agent, as described in Sections 10.2, 10.3, 11.6.1, and 11.6.3 of [1].

(2) Home Test Init and Home Test messages that pass through the home agent on their way to a correspondent node, as described in Section 10.7 of [1].

(3) ICMPv6 messages exchanged between the mobile node and the home agent for the purposes of prefix discovery, as described in Sections 10.9.3., 11.3.3, and 11.3.4 of [1].

The nodes MAY also optionally protect payload traffic passing through the home agent, as described in Section 5.3 of [1].

Signaling between the mobile node and the home agent requires message authentication, integrity, correct ordering and replay protection. The mobile node and the home agent must have an security association to protect this signaling.

Mobile IPv6 base document defines the main requirements the mobile nodes and home agents must follow when securing the above traffic. This draft 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 5. Section 6 describes rules which associated Mobile IPv6, IPsec, and IKE implementations must observe. Section 7 discusses how IPsec can be configured to use either manual or automatically established security associations. Section 8 shows examples of how packets are processed within the nodes.

All implementations of Mobile IPv6 mobile node and home agent MUST support the formats described in Section 5 and obey the rules in Section 6.

5. Packet Formats

In this section we describe the order of headers within the protected and tunneled packets over the wire. Support for the described ordering is mandatory for nodes that implement Mobile IPv6 mobile node or home agent functionality.

5.1. Binding Updates and Acknowledgements

When the mobile node is away from its home, the BUs sent by it to the home agent MUST have 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 or AH header
Mobility header
   Binding Update
```

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

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

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

```
IPv6 header (source = home agent, destination = home address)
ESP header or AH header
Mobility header
```

Binding Acknowledgement

5.2. Return Routability Signaling

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

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

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

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

Note that these formats rely on the SA destination address (tunnel gateway address) to change for the mobile node as it moves. This is discussed further in the requirements in Section 6.

5.3. Prefix Discovery

If IPsec is used to protect prefix discovery, requests for prefix from the mobile node to the home agent MUST have 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 or AH header
ICMPv6
   Mobile Prefix Solicitation
```

Again if IPsec is used, solicited and unsolicited prefix information advertisements from the home agent to the mobile node MUST have 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 or AH header
ICMPv6
   Mobile Prefix Advertisement
```

5.4. Payload Packets

If IPsec is used to protect payload packets tunneled to the home agent from the mobile node, a similar format is used as in the case of tunneled Home Test Init messages. However, instead of the Mobility Header these packets may contain any legal IPv6 protocol(s), and it is possible to use both AH and ESP for the protection:

```
IPv6 header (source = care-of address, destination = home agent)
ESP header or AH header
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 IPsec protection, they MUST have at least the following headers in the following order:

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

6. 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.

We will start with the main requirements:

- IPsec protection for Binding Updates and Acknowledgements between the mobile node and home agent MUST be supported and MUST be used.

- IPsec protection for the Home Test Init and Home Test messages tunneled between the mobile node and home agent MUST be supported and SHOULD be used.

- IPsec protection for the ICMPv6 messages related to prefix discovery MUST be supported and SHOULD be used.

- IPsec protection of the payload packets tunneled between the mobile node and home agent MAY be supported and used.

- Manual configuration of security associations MUST be supported and dynamic establishment MAY be supported.

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

- When ESP is used for protecting ICMPv6 or Mobility Header messages, a non-null authentication algorithm MUST be applied.

- When ESP is used for protecting tunneled Home Test Init and Home Test messages, a non-null encryption algorithm and non-null authentication algorithm MUST be applied.

- If replay protection is required, dynamic keying MUST be used. IPsec can easily provide replay protection only if dynamic keying is used. This may not always be possible, and manual keying would be preferred in some cases. 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 ensure correct ordering. However, if a home agent reboots and loses its state regarding the sequence numbers, replay attacks become possible. The use of a key management mechanism together with IPsec can be used to prevent such replay attacks.

- IPsec AH authenticator calculation MUST be performed as if a packet with a Type 2 Routing header would have the home address in the IPv6 destination address field and the care-of address in the Routing header. Type 2 Routing header should be treated by IPsec in the same manner as Type 0

Routing header.

- Similarly, the authenticator calculation MUST be performed as if a packet with a Home Address destination option would have the home address in the IPv6 source address field and the care-of address in the destination option.

- When a packet is matched against IPsec security policy or selectors of a security association, an address appearing in a Home Address destination option MUST be considered as the source address of the packet.

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

- When IPsec is used to protect return routability signaling or payload packets, the security association between the home agent and the mobile node MUST change its destination address (tunneled gateway address) when the care-of address for the mobile node changes. At the home agent, this modification takes place when a the care-of address in a binding changes. At the mobile node, this modification takes place immediately after movement.

- When IPsec is used to protect return routability signaling or payload packets, the security policy database entries SHOULD be defined specifically for the tunnel interface between the mobile node and the home agent. 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 following rules apply to mobile nodes:

- 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.

- If IPsec is used to protect return routability signaling or payload packets tunneled via the home agent, IPsec tunnel mode encapsulation MUST be used.

- Depending on whether IPsec AH or ESP is used the protection offered for the Binding Updates is slightly different. AH protects also the IPv6 header and any extension headers. It is important for the home agent to verify that the care-of address has not been tampered. If ESP is used, the IPv6 header where this information resides could potentially have been modified by attackers on the path. 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 when ESP is used, or when the implementation does not know whether AH or ESP is used.

- Where dynamic keying is used, the key management protocol MUST use the care-of address as the source address in the protocol exchanges.

- Conversely, the IPsec SAs MUST be requested from the key management protocol with the home address as the mobile node's address.

The following rules apply to home agents:

- 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.

- If IPsec is used to protect return routability signaling or payload packets tunneled to and from the mobile node, IPsec tunnel mode encapsulation MUST be used.

- We need 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 SA for any given home address and home agent when manual keying is used. When dynamic keying is used, the security policy database entries MUST unequivocally identify the IKE phase 1 credentials which can be used to create security associations for a particular home address.

7. 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. Our examples assume the use of ESP, but a similar configuration could also be used to protect the messages with AH.

Section 7.1 introduces the format we use in the description of the SPD and the SAD. Section 7.2 describes how to configure manually keyed security associations, and Section 7.3 describes how to use dynamic keying.

7.1. 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> |
  "IF" <condition> "THEN CREATE" <pattern> |
```

Where <condition> is an boolean expression about the fields of the IPv6 packet, <sa> is the name of an SA, and <pattern> is a specification for an SA to be negotiated via IKE. 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> "," <ahesp> "," <mode> ")"
":"
                    <selectors>
```

Where <dir> is "IN" or "OUT", <spi> is the SPI of the SA, <destination> is the destination of the SA, <ahesp> is either "AH" or "ESP", <mode> is either "TUNNEL" or "TRANSPORT", and <selectors> is a boolean expression about the fields of the IPv6 packet.

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".

7.2. Manual Configuration

7.2.1. Binding Updates and Acknowledgements

Here are the contents of the SPD and SAD for protecting Binding Updates and Acknowledgements in the mobile node mobile node and home agent home agent:

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

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

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

7.2.2. 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:

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

  mobile node SPD IN:
    - IF interface = tunnel from home_agent_1 & source = any &
         destination = home_address_1 & proto = MH
      THEN USE 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, home_address_1, ESP, TUNNEL):
      source = any & destination = home_address_1 & proto = MH

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

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

  home agent SAD:
    - SA4(OUT, spi_d, home_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
```

7.2.3. Prefix Discovery

In the following we describe some additional SPD and SAD entries to protect prefix discovery.

```
  mobile node SPD OUT:
    - IF source = home_address_1 & destination = home_agent_1 &
         proto = ICMPv6
```

```
          THEN USE SA5.

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

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

Note that the SPDs described above protect all ICMPv6 traffic between the mobile node and the home agent.

When new prefixes are advertised by the home agent, the MN MAY configure additional new home addresses. There may be a need to create new security associations, if the mobile node intends to use any of these home addresses to send a Binding Update to the home agent.

7.2.4. 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 = tunnel to home_agent_1 & source =
home_address_1 &
```

```
              destination = any & proto = X
           THEN USE SA7

       mobile node SPD IN:
         - IF interface = tunnel from home_agent_1 & source = any &
```

```
              destination = home_address_1 & proto = X
           THEN USE 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, home_address_1, ESP, TUNNEL):
           source = any & destination = home_address_1 & proto = X

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

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

       home agent SAD:
         - SA8(OUT, spi_h, home_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
```

7.3. Dynamic Keying

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

7.3.1. 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 CREATE ESP TRANSPORT SA: local phase 1 identity = user_1

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

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

       home agent SPD IN:
```

- IF source = home_address_1 & destination = home_agent_1 & proto = MH
  THEN CREATE ESP TRANSPORT SA: 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 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't 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 isn't 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 certificate authority.

7.3.2. Return Routability Signaling

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

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

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

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

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

One difference to the above is that we specified the tunnel gateway address, as we need to use a different address for that than those appearing in the packets.

7.3.3. 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 CREATE ESP TRANSPORT SA: local phase 1 identity = user_1

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

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

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

7.3.4. 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 = tunnel to home_agent_1 &
         source = home_address_1 & destination = any & proto = X
      THEN CREATE ESP TUNNEL SA: gateway = home_agent_1 &
                                 local phase 1 identity = user_1

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

  home agent SPD OUT:
    - IF interface = tunnel to home_address_1 &
```

```
       source = any & destination = home_address_1 & proto = X
    THEN CREATE ESP TUNNEL SA: gateway = home_address_1 &
                               peer phase 1 identity = user_1

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

7.4. Mobile Node Returning Home

When the MN returns home and deregisters with the Home Agent, the tunnel between the home agent and the MN's CoA is torn down. The SPD entries, which were used for protecting tunneled traffic between the MN and the HA become inactive. The corresponding SAs could be stored or deleted depending on how they were created. If the SAs were created dynamically using IKE, they are automatically deleted when they expire. If the SAs were created through manual configuration, they can be retained and used later if the MN moves aways from home.

The SAs created for BU/BA protection SHOULD not be deleted as they do not depend on care-of addresses and can be used again.

8. Processing Steps within a Node

In this section we give examples of what processing steps node can take to achieve the required packet formats and satisfy the requirements. These example are for illustration purposes only, and implementations are free to choose other strategies as long as the results stay the same on the wire.

8.1. 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 policy data base 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 11.2.2 in [1]. 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
```

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
```

8.2. 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 SA selectors (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.

8.3. 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 9.6 in [1]. 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
```

8.4. 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 SA selectors (source = home agent, destination = home address, proto = MH).

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

8.5. 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 no longer satisfies the criteria that made it enter the tunnel, and it is sent directly to the home agent.

8.6. 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 selectors and the packet can be processed further.

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

8.7. 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 gateway 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 no longer satisfies the criteria that made it enter the tunnel, and it is sent directly to the care-of address.

8.8. 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 SA selectors (source = any, destination = home address).

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

8.9. Prefix Solicitation Message to the Home Agent

This procedure is similar to the one presented in Section 8.1.

8.10. Prefix Solicitation Message from the Mobile Node

This procedure is similar to the one presented in Section 8.2.

8.11. Prefix Advertisement Message to the Mobile Node

This procedure is similar to the one presented in Section 8.3.

8.12. Prefix Advertisement Message from the Home Agent

This procedure is similar to the one presented in Section 8.4.

8.13. Payload Packet to the Home Agent

This procedure is similar to the one presented in Section 8.5.

8.14. Payload Packet from the Mobile Node

This procedure is similar to the one presented in Section 8.6.

8.15. Payload Packet to the Mobile Node

This procedure is similar to the one presented in Section 8.7.

8.16. Payload Packet from the Home Agent

This procedure is similar to the one presented in Section 8.8.

9. Implementation Considerations

We have chosen to require an encapsulation format for return routability and payload packet protection which can only be realized if the IPsec implementation can be controlled via an API. 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. The API should minimally support changing the gateway address of a security association towards the mobile node as the mobile node moves. Implementations are free to choose other methods to update a security association. This includes deleting the current SA and adding a new SA.

We have also chosen to require that a dynamic key management protocol must be able to make an authorization decision for IPsec SA 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.

The base Mobile IPv6 specification 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 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).

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.

10. Security Considerations

The Mobile IPv6 base specification [1] requires strong security between the mobile node and the home agent. This memo discusses how that security can be arranged in practise, using IPsec.

11. References

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support for IPv6", Internet Draft draft-ietf-mobileip-ipv6-19.txt. (Work In Progress.) September 2002.

[2] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol" RFC 2401, BBN Corp, @Home Network, November 1998.

[3] D. Harkins and D. Carrel, "The Internet Key Exchange", RFC 2409, Cisco Systems, November 1998.

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

12. Acknowledgements

The authors would like to thank Erik Nordmark, Gabriel Montenegro, Kevin Miles, Cheryl Madson and Jari T. Malinen for interesting discussions in this problem space.

13. Author's Address

Jari Arkko
Oy LM Ericsson Ab
02420 Jorvas
Finland

EMail: Jari.Arkko@ericsson.com

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

EMail: vijayd@iprg.nokia.com

Francis Dupont
ENST Bretagne
Campus de Rennes 2, rue de la Chataigneraie
BP 78
35512 Cesson-Sevigne Cedex
France

EMail: Francis.Dupont@enst-bretagne.fr