Network Working Group
Internet-Draft
Intended status: Informational
Expires: November 1, 2009

A. Ebalard
EADS

April 30, 2009

Mobile IPv6 Home Link Detection Mechanism Security considerations
draft-ebalard-mext-hld-security-00

Status of this Memo

Copyright Notice

Abstract

MIPv6 defines the concept of Home Network for a MN, in opposition to the foreign network where this entity may find itself. A ``Home Link Detection'' mechanism is also specified to allow the MN to detect

when it is at home.

MIPv6 specification mandates the use of IPsec for protecting main signaling traffic and also defines how IPsec can be used to protect data traffic between the MN and its HA. Even if optional, it is expected that many deployments of MIPv6 will use it by default for MN which may roam outside a trusted infrastructure (e.g. outside a mobile operator network).

When a MN detects it is at home, it is expected to stop IPsec protection for data traffic exchanged with its Home Agent. That event is the result of the Home Return procedure, triggered by the Home Link Detection mechanism.

This document discusses the possible threats and security impacts associated with the use of this insecure NDP-based mechanism as a trigger to drop IPsec protection of data traffic for the MN. It also provides some results on the implementation of the attacks against an existing MIPv6 module. Possible solutions are suggested.

Table of Contents

1. Keywords

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Scope and Hypothesis

2.1. Scope

MIPv6 entities (MN and HA) perform Neighbor Discovery Protocol exchanges, for various needs:

- the HA: acting as a ND proxy for registered MN which are currently in a foreign network, the HA defends the MN's HoA on the MN's Home Link when it is away, intercepts packets destined to the HoA and tunnels them to the associated MN at its CoA. Its operations as a ND Proxy for MN's HoA are basically subject to the same ND threats as the ones existing for common neighbors of the link. Those are not covered in the document.

  In practice, additional hypothesis can be made about the Home Network; Being part of a controlled infrastructure, those threats can be reduced, mitigated or avoided.

  As discussed in next item dedicated to the MN, those hypothesis can usually not be made about the foreign networks where the MN operates.

- the MN: upon movement, the MN performs link layer interactions with the new foreign network it finds itself in. By default, from a security standpoint, those foreign networks must be considered as hostile environments (i.e. with possible attackers). This hypothesis may be relaxed in specific deployments where the MN is expected to roam only between trusted networks (e.g. mobile operator networks). We do not consider these relaxed/specific hypothesis in the document.

  The interactions of the MN on foreign networks can be summarized the following way: it sends RS messages in order to get some RA from the router(s) of the link. The RA gathered during the router discovery steps are used by the MN to configure a CoA and most importantly to detect if the current link is the home link or a foreign link.

  For that reason, the MN in this potentially hostile environment is subject to ND protocol threats, already described in [RFC3756].

  But because the Home Link detection mechanism is based on information gathered using NDP and may be the trigger for some additional critical security steps, it may be a vector for additional MIPv6 threats.

Specifically, this document focuses on the MIPv6-specific link layer security issues associated with home link detection (and Home Return procedure). It discusses the possible security issues associated with current definition of those mechanisms, lack of security considerations on those mechanisms and inacurracies in reference documents.

2.2. Hypothesis

For the reasons introduced in Section 2.1, one important hypothesis made in the document is that tunneled traffic (data and possibly some specific signaling messages) is protected using IPsec in tunnel mode, even if not mandated by the reference documents. Some arguments justify this decision:

- The Home Agent and the Mobile Node belong to a common trust domain, and are already expected to support IPsec and share common

credentials for protecting signaling with IPsec in transport mode. In that context, supporting tunnel mode is expected to be inexpensive from a deployment standpoint. The main remaining point in this discussion is the possible performance cost of handling IPsec protected data traffic in the home network.

- As specified in [RFC3776] and [RFC4877], ``Tunnel mode IPsec ESP MUST be supported and SHOULD be used for the protection of packets belonging to the return routability procedure''.
- Protection of IPsec payload traffic is documented for both static and dynamic keying with IKEv1 [RFC3776] and IKEv2 [RFC4877]. Various implementations are known to support it.
- Except for specific devices which will operate on some trusted operator or internal networks, Mobile Nodes are expected to find themselves in untrusted/hostile foreign networks. In that context, corporate deployments will require the use of IPsec for tunneled data. Public deployments will also probably follow that path.

In the end, as discussed later in this section, IPsec tunneling and common (IPv6-in-IPv6) tunneling of data are basically handled in the same way with regard to home return.

The rest of the document discusses the possible issues associated with current Home Link Detection mechanism and ``Returning Home'' procedure as specified in the main MIPv6 reference documents ([RFC3775], [RFC3776], [RFC4877], [draft-ietf-mext-rfc3775bis], and

[RFC5026]).

As described previously, this is done under the hypothesis that IPsec is used to protect the traffic exchanged between the Mobile Node and its Home Agent.

3. Mechanisms overview

To keep current section a reasonable size, the detailed analysis of reference documents including normative excerpts of those specifications is maintained in Appendix A, at the end of the document. If you are interested by more details on the topic, you should definitely read that appendix.

Here, we provide an overview of:

- The Home Link Detection mechanism performed by the MN
- The events associated with the ``Returning Home'' procedure on both the MN and the HA.

It is based on the detailed analysis available in the appendix.

3.1. Home Link Detection mechanisms overview

The MIPv6 specification provides a simple (one would say primitive) Home Link detection mechanism for the MN: simply put, when a Prefix Information Option found in a RA message received by the MN includes its Home Subnet prefix, the MN considers it is on its Home Link.

3.2. Returning home events overview

The reaction of the MN to previous event (detection of home network) is defined, but in a loose fashion:

- It is expected to send a deregistration BU: the content of the BU is provided by [RFC3775] (the set of flags in MH header) but the specific format of the packet is just suggested (no HAO and no AltCoA option). In practice, the document does not prevent an implementation to include an AltCoA option or a Destination Option Header carrying a Home Address Option (HAO).
- [RFC3775] precisely describes the steps that should then occur at ND level, in order for the MN to be able to use its HoA, which was previously defended by the HA. We do not cover those steps here.
- [RFC3775] expects the tunnel with the HA to be torn down. [RFC3776] also follows that direction by expecting the IPsec tunnel with the HA to be torn down. In practice, this is what existing implementations do.

- The specific order in which things are expected to happen is unclear, and more or less left as an implementation decision despite its importance: the MN may not wait for the BA to come back from the HA in order to tear its IPsec tunnel down; just like it may not wait (for obvious latency reasons) for a BA to come back to update its IPsec tunnel SP/SA when performing a handover to another foreign network.

4. Theoretical threats

The security aspects of the Home Link Detection mechanism and ``Returning Home'' procedure are not covered in any of the MIPv6 reference documents. Those are basically not considered as possible threat vectors. One possible reason for that may be the fact that protection of data traffic (authentication, privacy, ...) is not considered in the documents (support and use of IPsec for that purpose is optional). MIPv6 reference documents focus on the protection of the infrastructure (address ownership considerations, ...) but not on security of user traffic.

4.1. Full deregistration attack

Here, we discuss the possible threats associated with the loose expectations of reference documents and the reliance on untrusted information to trigger changes in tunneling and IPsec security policies.

The only document which considers the topic is [draft-haddad-mext-mip6-residual-threats], which has an interesting Section 5 entitled ``Exploiting Neighbor Discovery in a MIPv6 Environment''. That section being quite short, it is provided (text is extracted from current version, i.e. version 2) here for completeness and commented below as an initial introduction to the possible threats:

...

This threat offers a malicious node two edges. It requires first that the attacker be attached to the same foreign link as the MN, and the discovery of the MN's home agent IP address as well as the MN's IP home address (which may not pose a serious problem). After learning these two information, the attacker advertises the MN's home prefix on the link thus leading the MN to believe that it has returned to its home network. Such information will prompt the MN to send a BU message to its HA to request de-registration. However, such early de-registration may not be possible as the foreign network may have activated ingress filtering. But the main goal for the attacker is to get a valid copy of the MN's BU message and such goal is achieved. If the malicious node concludes that the MN is still receiving data packets tunneled by the HA to its current CoA, then it will get involved in the MN de-registeration procedure by forwarding the BU message to the MN's HA on another interface where ingress filtering is not activated (i.e. under the assumption that the attacker is multihomed). Upon receiving the BU message, the HA will de-register the MN and stops tunneling data packets to the MN's CoA. In addition, the HA sends back a BA message which will never reach the MN. From that moment, the data traffic sent by the CN(s) stops at the MN's home network. However, the lack of ACK messages sent by the MN will prompt the CN(s) at some point to halt sending data traffic and eventually tear down the session(s).

However, the situation gets worse if the malicious node decides to push further in his attack by sending fake ACK messages to the CN(s), i.e. using the MN's home address. In such situation, the CN(s) will keep sending data traffic to the MN's HA (where they eventually get discarded) and thus, may cause severe disruption within the home access network, possibly leading to a network flooding attack in some specific topologies.

Note that as they may be more than one MN attached to the same foreign link and using the same home prefix, such attack may lead to collective de-registration.

...

As discussed in the draft and predicted by the summary provided previously, it is expected to be quite easy for an attacker on a foreign link to have a MN think that it is at home and have it send a de-registration BU. For that purpose, as noted in the draft, the attacker only needs to acquire the Home Agent address, its Home

Prefix and have the ability to forge packets. The addresses are public information available from the traffic of the MN.

The draft introduces the possibility that ingress filtering implemented in the foreign network could lead to the BU being dropped before hitting the HA.

In fact, for a common HAO-free deregistration BU packet sent by a MN to its HA while believing it is at home, the source address of the packet is the HoA. With that hypothesis, the packet is both topologically invalid from the foreign network's perspective (it should be dropped if some filtering mechanism has been put in place by the ISP of the foreign site or even the administrator of the site), but it is also invalid from the destination site's perspective (it should definitely be dropped at the MN's network site boundaries). But those expectations do not provide any real security guarantees.

The solution proposed in the draft for the attacker is to relay its packets via another connection mean which does not undergo ingress filtering. It is interesting to note that it will still not work if the Home Network implements ingress filtering too, and the attacker (and the MN) will never get a Binding Ack in response. The only way for an attacker would be to have a simultaneous access to the MN's foreign network and to its home network.

Let's be wild and consider for a moment that an implementation does not have restrictions (both from the MN packet build perspective and the HA processing perspective) on the expected format of the BU. This could be the case because of code reuse. In that context, there are some paths the attacker may explore. For instance, if the attacker manages to get access to the ESP protected deregistration BU sent by the MN in its expected common format (while believing it is at home):

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

It could simply modify the packet in the following way to add a destination option header with an HAO to make it look that way:

```
IPv6 header (source = Attacker_Address,
             destination = HA address)
Destination Options header
   Home Address option (HoA)
ESP header in transport mode
Mobility header
   Binding Update
```

The packet is still perfectly valid at all levels:

- The part protected by ESP has not been modified during the addition so it should still be gracefully processed by the HA IPsec stack. It is expected that the processing of the HAO be performed before the IPsec processing, hence replacing the attacker address (Attacker_Address) by the HoA.
- Mobility Header checksum is computed based on MH content (which has not been modified) and using the usual L4 pseudo header which is also the same after the changes: the final addresses are still the HoA and the Home Agent address, the next header field is still MH. The last element of the pseudo header, the length of the upper layer is not bound to the modified payload length field of the IPv6 header but to the unchanged length field of the MH header.

In the end, the mangled packet now has a more interesting layout: it has a topologically valid source address which will allow it to be routed to the HA. For previous reasons, it should be processed successfully by the IPsec stack of the HA and delivered to its MIPv6 module. Then, whether it will be considered valid by the HA is a matter of implementation and interpretation of the reference documents. Among the remaining questions/points, we can list the following:

- There is no AltCoA in the packet: in our example, there is none. But, here again, reference documents are not clear on the topic. AltCoA is usually expected in BU to benefit from the IPsec protection. But there are specific non normative notes in [RFC3775] and [RFC3776] for deregistration BU sent from Home: usual ones do not include the AltCoA option. This point is mainly

left as an implementation issue. For instance, the Mobile IPv6 implementation for Linux (UMIP) always includes the AltCoA option, even for deregistration BU sent when back home.

- Under the assumption that the HA processes the BU, can we expect it to send the BA in the same fashion, using a RH2? This is clearly implementation dependent. From a specification point of view, the BA is expected to be always sent to the source address of initial packet. In our example, Attacker_Address.

- Will the attacker be able to mangle received BA and have it be processed by the MN? For the same reasons as the ones given above, this may be possible.

As a temporary summary, the specific implementation of the MIPv6 module running on the MN and the HA, the kind of filtering implemented in the foreign and home networks will impact the difficulty and requirements of setting up a full BU/BA exchange leading to a complete deregistration on both sides.

4.2. Partial deregistration

It is interesting to note that the final goal of the attacker may not be to mount a full deregistration attack, but to have the MN drop its IPsec tunnel protection. In that context, a full attack would obviously do the job but some less difficult solutions may exist.

For instance, the reference documents leave quite some latitude with respect to the order of events. For obvious performance reasons, it is common for a MIPv6 modules not to wait for the BA from its HA to start using its new address. In the context of the deregistration when coming back home, the MN may drop its IPsec tunnel protection early, just after sending its BU and before receiving the BA. Mobile IPv6 for Linux implementation (UMIP) can be configured to do that.

4.3. Conclusion

As a conclusion, the Home Link Detection mechanism rely on untrusted and spoofable ND information. It is used as a trigger for a significant security event when IPsec is used for protecting data between the MN and its HA: the removal of this IPsec tunnel protection on a foreign network.

Moreover, various parts of the reference documents leave quite some room for the build and processing of packets and the order of events associated with deregistration and Home Return. It may lead to interoperability issues and may also simplify the work of an attacker which intend to exploit previous flaws.

From our standpoint, when IPsec is used to protect data traffic, even if an attacker manages to access the Home Subnet of a MN, this should not provide her the ability to have one such MN drop its IPsec protection on a foreign network. At the moment, current MIPv6 reference documents may allow that to happen.

5. Implementing the attacks: PoC against UMIP

This section documents the implementation of the attacks described in previous section against an existing implementation. The targeted implementation is UMIP, the freely available Linux implementation.

The tool used to implement the attack in order to create or mangle MIPv6 packets is Scapy.

5.1. MN's configuration and behavior

In this section, a Linux MN running UMIP is considered, configured in order for signaling and data traffic to be IPsec-protected. The former undergoing transport mode protection and the latter tunnel mode protection.

One configuration parameter of interest in the following discussions is OptimisticHandoff option. It has the following description in the software man page:

> When a Mobile Node sends a Binding Update to the Home Agent, no Route Optimized or reverse tunneled traffic is sent until a Binding Acknowledgement is received. When enabled, this option allows the Mobile Node to assume that the binding was successful right after the BU has been sent, and does not wait for a

positive acknowledgement before using RO or reverse tunneling.

Even if the option is disabled by default it is useful to limit the effect of the RTT between the MN and its HA when performing a handover. For that reason, chances are high client will enable it.

It should be noted that the effect of the option is (unintentionally?) different whether the MN performs a movement to a foreign network or to the home network.

In former case, when the option is enabled, directly after sending its BU, the MN migrates the tunnel endpoint of its tunnel mode IPsec SP/SA (and warns the IKE daemon of the change of CoA) as usual but also removes a blocking rule for traffic which would normally be kept until the BA is received. From the user perspective, the switch has already happened, even if the HA has not yet acknowledged it with a BA.

In latter case, when the option is enabled, all the changes required for the direct unprotected communication of the MN on its Home Link are done directly after the emission of the BU. Nonetheless, a rule which prevents packets sent from the HoA to flow remains until the protected BA is received from the HA. In the end, while waiting for

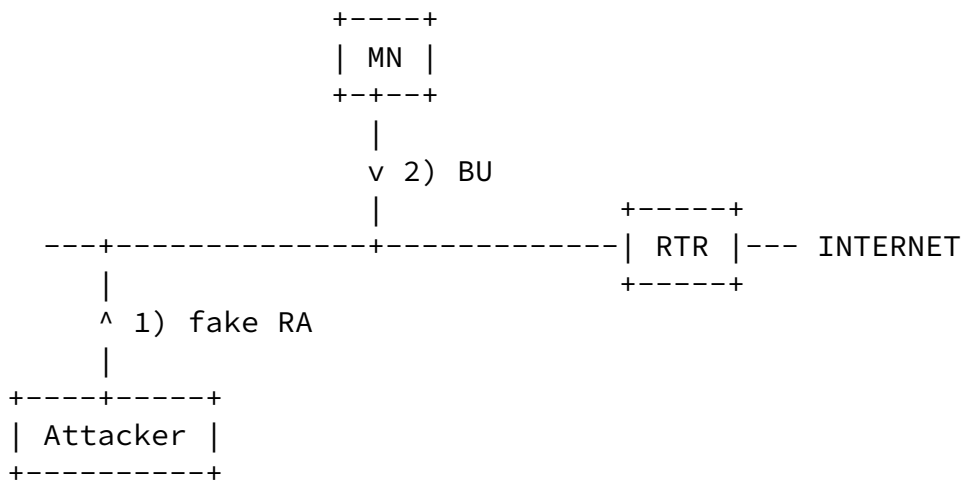
the BA, the MN does process unprotected traffic sent to its HoA but is unable to reply (i.e. sent traffic back from its HoA).

Previous behavior when the OptimisticHandoff option is enabled deserves some comments:

- Considering the latency argument (RTT of the BU/BA exchange) does not hold when the MN comes back home, the fact that UMIP also performs a optimistic handoff in this situation looks like a bug or at least a bad idea.
- The rule preventing traffic from the HoA until the reception of the BA seems inconsistent with the rest of the code (it may be here by luck).

5.2. Attacker announcing a MN's Home Network Prefix

This subsection documents the effect on a UMIP-based (IPsec-protected) MN of an attacker injecting fake RA, advertising the Home Network Prefix (and the Home Agent address).



As introduced in previous subsection, the behavior of an UMIP MN vary based on the value of the OptimisticHandoff configuration parameter. If it is disabled (the default), the MN is unable to communicate before the IPsec protected BA is received from the HA. In that case, the attack results in a DoS, but does not allow the attacker to directly send traffic to node or access traffic sent by the node.

When the OptimisticHandoff option is enabled, reception of the RA advertising the Home Network prefix of the MN directly leaves the MN without IPsec protection on the attacker's link. As covered in previous subsection, a residual blackhole route which is only dropped after the reception of the BA by the MN prevents it to leak data packets. Nonetheless, even if it is unable to reply, the MN will happily process packets sent to its HoA (to listening UDP services for instance).

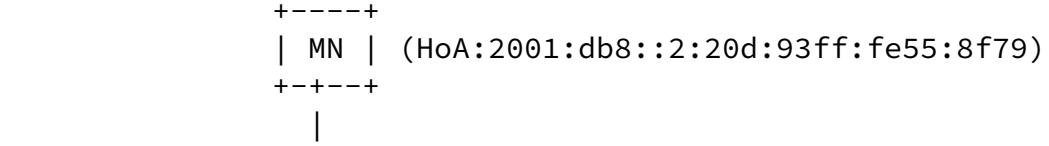
5.3. Attacker relaying BU/BA via HAO/RH2 addition

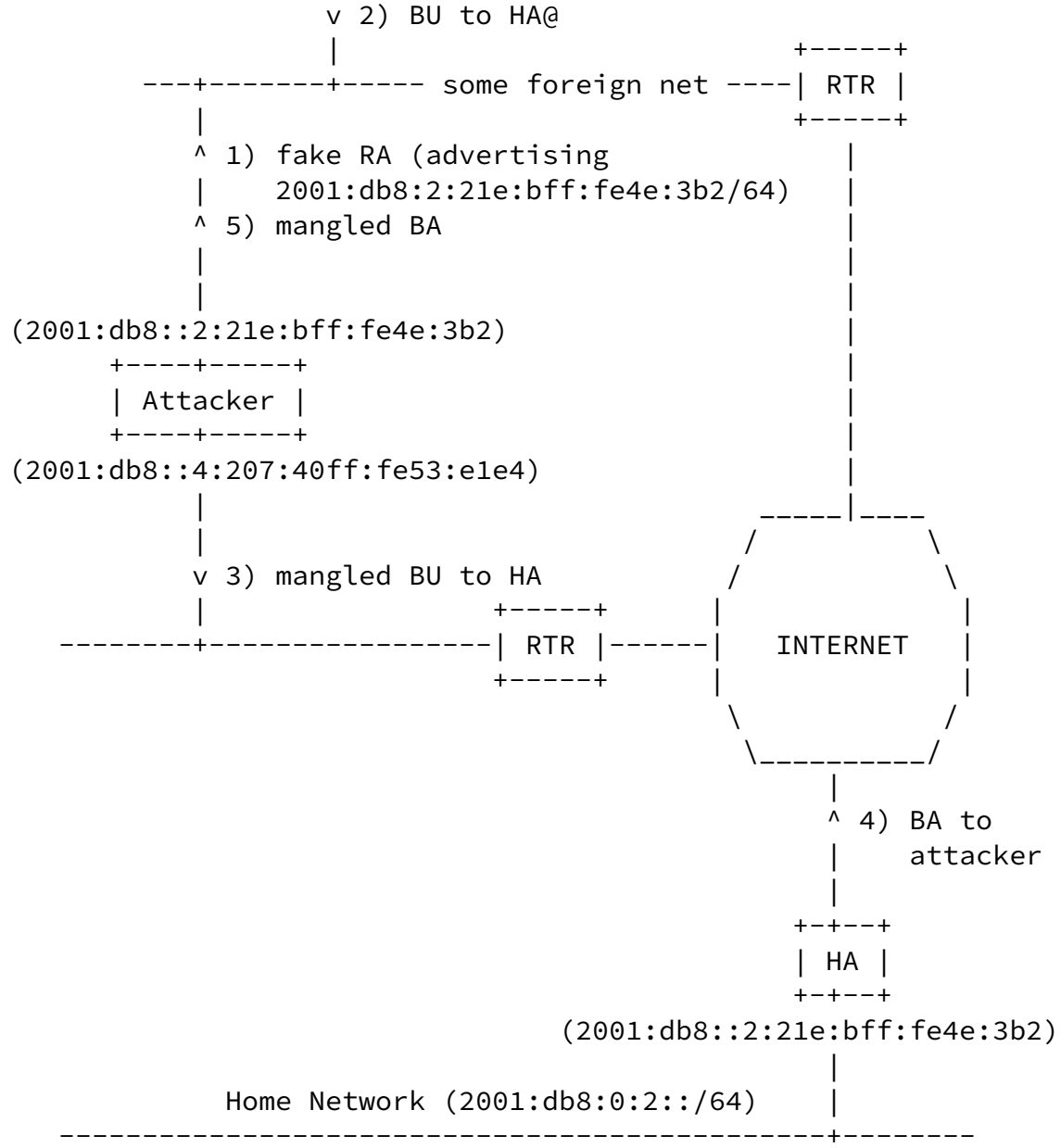
As described in previous subsection, an attacker only advertising the Home Network Prefix to an UMIP MN may be able, depending on the specific configuration of the peer, to have it drop the IPsec tunnel protecting data traffic.

At most, in the best software configuration for the attacker (OptimisticHandoff enabled on the MN), this may allow it to have traffic sent to the peer on its HoA. The inability for the MN to send traffic back from the HoA (blackhole rule installed until the

reception of the BA) will prevent TCP connection to happen.

Now, as explained in the first part of the document, the attacker can improve the attack by mangling ESP-protected deregistration BU sent by the peer (to the attacker, which the MN believes to be its HA) and then resend it to the HA. The setup is depicted on the following picture:





The attacker now has two interfaces (it may be possible to mount the attack with one interface but this is not presented for clarity reasons), one on which it interacts with the MN and the other which it uses to send/receive packets to/from the HA. On that second interface, its address (used in following descriptions) is 2001:db8::4:207:40ff:fe53:e1e4.

The HA is available at 2001:db8::2:21e:bff:fe4e:3b2, the Home Subnet

of the MN being 2001:db8:0:2::/64. The MN's HoA is 2001:db8::2:20d:93ff:fe55:8f79.

Extending the code developed for previous attack basically involves mangling the packet in the following way (Scapy/Python code):

```
  ...

  ipv6 = pkt[IPv6]     # access IPv6 layer from received packet
  esp  = ipv6.payload  # ESP-protected BU follows IPv6 layer
  ipv6.payload = None  # Remove IPv6 payload from packet
  del(lower.plen)      # Delete length to have it recomputed

  # Build HAO in DestOpt with NH set to 50 (ESP)
  hao      = HAO(hoa=ipv6.src)
  destopt  = IPv6ExtHdrDestOpt(options=[hao], nh=50)
  ipv6.src = attacker_addr # used to send packet

  # Set IPv6 NH value to DestOpt
  ipv6.nh = 60

  # Result is made of mangled IPv6 pkt, followed by Destination
  # Option header carrying the HAO, followed by the (unchanged)
  # ESP-protected BU
  p = ipv6 / destopt / esp

  ...
```

For clarity, the ESP-protected BU received by the attacker from the MN after having sent the RA and announced itself as the MN's HA has the following layout:

```
  ###[ IPv6 ]###
       version= 6L
       tc= 0L
       fl= 0L
       plen= 84
       nh= ESP Header
       hlim= 64
       src= 2001:db8::2:20d:93ff:fe55:8f79
       dst= 2001:db8::2:21e:bff:fe4e:3b2
  ###[ ESP Extension Header ]###
          spi = 0x0990cbed
          seq = 3
          load= "\x97\xd2w\xadx9\x88\xa2\xba\x90\xcd\xd9\xa..."
```

The address of the MN is 2001:db8::2:20d:93ff:fe55:8f79. The address

of the HA is 2001:db8::2:21e:bff:fe4e:3b2.

The packet sent to the HA at the end of the mangling process associated with previous code has the following layout:

```
  ###[ IPv6 ]###
       version= 6L
       tc= 0L
       fl= 0L
       plen= 108
       nh= Destination Option Header
       hlim= 64
       src= 2001:db8::4:207:40ff:fe53:e1e4
       dst= 2001:db8::2:21e:bff:fe4e:3b2
  ###[ IPv6 Extension Header - Destination Options Header ]###
          nh= ESP Header
          len= 2
          autopad= On
          \options\
           |###[ PadN ]###
           |  otype= PadN [00: skip, 0: Don't change en-route]
           |  optlen= 2
           |  optdata= '\x00\x00'
           |###[ Home Address Option ]###
           |  otype= Home Address Option [11: discard+ICMP not mcast,
           |                                0: Don't change en-route]
           |  optlen= 16
           |  hoa= 2001:db8::2:20d:93ff:fe55:8f79
  ###[ ESP Extension Header ]###
             spi = 0x0990cbed
             seq = 3
             load= "\x97\xd2w\xadx9\x88\xa2\xba\x90\xcd\xd9\xa..."
```

Its source address is now the address of the attacker (2001:db8::4:207:40ff:fe53:e1e4) which provides it connectivity to the internet in order to reach the HA (the unmodified destination address found in the IPv6 header of the packet, i.e. 2001:db8::2:21e:bff:fe4e:3b2). The address of the MN (2001:db8::2:20d:93ff:fe55:8f79) is now found in the inserted Home Address Option. The ESP Extension Header has not been modified in the process. It should be noted that the payload length field of the IPv6 header has been recomputed by Scapy: its value differs from the one in the initial packet due to the

addition of the Destination Option Header.

Having implemented the mangling of the BU, the attacker expects the HA to reply (if the BU is accepted) with a BA. This BA, sent to the address of the attacker, will include a Type 2 Routing Header (RH2). Unlike previous mangling which required the insertion of an extension header in the packet (the Destination Option Header), the attacker now needs to remove the RH2 from the BA and set the MN's HoA as

destination address in the IPv6 header before sending it to the peer.

Improving the PoC to do that can be done in the following way:

```
    ...

    ipv6 = pkt[IPv6]     # access IPv6 layer from received packet
    rh2  = pkt.payload   # RH2 follows IPv6
    esp  = rh2.payload   # ESP follows RH2
    ipv6.payload = None  # Remove what follows IPv6 header
    del(lower.plen)      # Delete length to have it recomputed

    ipv6.dst=rh2.addresses[0] # Set HoA from RH2 as IPv6 dst address
    ipv6.nh = 50         # Update IPv6 next header field value

    p = ipv6 / esp

    ...
```

For clarity, the ESP-protected BA received by the attacker as a response from the HA has the following layout:

```
  ###[ IPv6 ]###
       version= 6L
       tc= 0L
       fl= 0L
       plen= 92
       nh= Routing Header
       hlim= 64
       src= 2001:db8::2:21e:bff:fe4e:3b2
       dst= 2001:db8::4:207:40ff:fe53:e1e4
  ###[ IPv6 Option Header Routing ]###
          nh= ESP Header
```

```
            len= 2
            type= 2
            segleft= 1
            reserved= 0L
            addresses= [ 2001:db8::2:20d:93ff:fe55:8f79 ]
      ###[ ESP Extension Header  ]###
               spi = 0x0cdede2b
               seq = 3
               load= '\xbd\x8aq\xb4\xfa\xccR\xfa\xa3Q\tf\x89...'
```

The packet obtained at the end of the mangling process associated with previous code has the following layout:


```
      ###[ IPv6 ]###
           version= 6L
           tc= 0L
           fl= 0L
           plen= 68
           nh= ESP Header
           hlim= 64
           src= 2001:db8::2:21e:bff:fe4e:3b2
           dst= 2001:db8::2:20d:93ff:fe55:8f79
      ###[ ESP Extension Header  ]###
                 spi = 0x0cdede2b
                 seq = 3
                 load= '\xbd\x8aq\xb4\xfa\xccR\xfa\xa3Q\tf\x89...'
```

As for previous mangling operation, the value of the payload length field in the packet has been automatically recomputed by Scapy to reflect the removal of the RH2.

5.4. Conclusion

5.4.1. Results

Implementing a PoC to test the effects of all theoretical attacks against UMIP was easily done by developing a small Automaton under Scapy (few lines of Python code).

With such a tool, an attacker simply advertising the Home Subnet prefix of a MN is able to make it believe it is at home. Depending on the configuration of the MN, this may allow the attacker to directly target the MN:

- If OptimisticHandoff configuration option is disabled (the default) this result in a simple DoS, the MN waiting for a BA before it is able to communicate.
- If OptimisticHandoff configuration option is enabled, the MN can then be joined on its HoA but cannot sent traffic from that address (i.e. reply for instance) until the reception of the BA.

When the attacker also activates the relaying of BU from the MN to the HA and the relaying of the associated BA from the HA to the MN, the attack gets effective: the MN is fully deregistered and does no more use IPsec protection for data traffic, believing it is on its home network.

The attack works against UMIP implementation because the values found in the source address of the IPv6 packet, the Home Address Option and the AltCoA are not invalid from a specification standpoint, for a de-registration BU.

Another reason is that the addition (respectively removal) of the Destination Option Header (respectively RH2) in the the BU (respectively BA) does not interfere with the protection provided by ESP on the signaling traffic.

5.4.2. UMIP improvements

In this subsection, we discuss the additional checks that UMIP should implement in order to prevent previous attacks. Note that those checks should only be seen as workarounds/improvements of current situation, but not as a complete solution to the Home Link Detection mechanism.

UMIP should not enforce an optimistic behavior when coming back home, i.e. it should not drop its IPsec tunnel protection before the BA is received from the HA. This does not make much sense from a performance point of view and has security impacts, leading to the ability for an attacker to have the MN handle incoming traffic (even though the MN is unable to reply until it receives the protected BA

from the HA).

UMIP should be modified in order for the HA to perform stricter checks on incoming BU and only allow the following layouts for de-registration BU:

- Case 1 (Home De-registration): Lifetime is set to 0, the packet does not contain an AltCoA option, does not contain a Destination Option Header carrying a HAO and has HoA as IPv6 source address.
- Case 2 (Remote De-registration): Lifetime is set to 0, the packet IPv6 source address is current registered CoA, the packet contains a Destination Option Header carrying a HAO (which contains the HoA), the packet contains an AltCoA option carrying current registered CoA (i.e. matching IPv6 source address of the packet).

Not that those proposed checks are stricter than the one expected from a RFC3775-compliant implementation which may result in interoperability issues. Ironically enough, if such strict layouts had been initially specified in the reference documents, this would have helped, both from interoperability and security standpoints.

As detailed in the appendix, the rules for MN and HA for the creation and processing of BU are more than fuzzy in reference documents. Those are spread over at least 4 sections of [RFC3775]: 6.1.7, 9.5.1, 10.3.2, 11.7.1. Rules for the sender (MN) and the receiver (HA) do not match on some aspects, for no specific reasons.

6. Workarounds and solutions

In this subsection, we discuss some possible leads for solving the issue presented in the document.

6.1. Improve reference documents consistency

Without considering here the security impacts of current Home Link Detection mechanism (discussed in following subsections), current MIPv6 specification (and also [draft-ietf-mext-rfc3775bis]) would need some work in order to define BU/BA processing/handling in a more precise and consistent way.

For instance, the allowed format of de-registration BU (AltCoA option, HAO in Destination Option Header, IPv6 source address, ...) should be precisely described for both cases (home and remote de-registration) instead of relying on information from different sections. This would both help in the development and security review.

6.2. Use of SEND in Home Link Detection mechanism

The first idea that comes to mind is to try and work on the root of the issues, the Home Link Detection mechanism. By removing an attacker the ability to spoof RA on a foreign network with crafted ones including PIO with Home Subnet Prefix, the issue could possibly be prevented.

For that purpose, from a theoretical standpoint, SEND could directly be used, simply by creating a Secure Home Link Detection mechanism in which it would be required that RA advertising the Home Subnet Prefix be signed. That way, an attacker on a foreign link would not be able to trigger a deregistration and this would prevent the IPsec tunnel protection to be dropped.

It should be noted that this possible solution comes with the following drawbacks:

- It requires SEND to be implement on the Home Network.
- It requires SEND to be supported by the MIPv6 module.
- It does not protect the MNs on a foreign link against an attacker that has simultaneous access to both the MN's Home Subnet and the MN's foreign subnet. Even if this is a strong hypothesis.

6.3. Never drop IPsec tunnel protection

MIPv6 specification does not mandate the removal of the tunneling between the MN and the HA. [RFC3776] and [RFC4877], even if they

expect the IPsec tunnel to be torn down when back home, do not mandate it either.

It is possible to solve the issue by having MN warning their HA that they are not willing to drop their IPsec tunnel when back home. This

simple solution (indicating that willingness to keep IPsec tunnel protection up and running on the home subnet is just a matter of a single flag in a BU) would provide an efficient workaround to the issue.

It would also be possible not to advertise anything in the BU (not consume a flag) and let that as a local configuration issue between the MN and the HA (requiring configuration to be in sync on both sides).

One would argue that this solution (maintaining IPsec tunneling on the Home Network) could have negative drawbacks on performance.

6.4. No home network

The last obvious and most simple solution to the issue is basically another a variant of previous proposal (``Never drop IPsec tunnel protection''), but this time by removing the ability for the MN to come back home (i.e. remove the concept of Home Network for a MN) and consider the home network is virtual.

7. IANA Considerations

This section is purposely kept empty.

8. Security Considerations

The whole document discusses security considerations on the Home Link Detection mechanisms defined in [RFC3775]. It covers the implication of its use when IPsec is used to protect data traffic (as allowed/ expected by reference documents).

Expected format and handling of BU/BA by HA/MN are discussed from a security perspective.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3776] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

9.2. Informative References

[draft-haddad-mext-mip6-residual-threats] Haddad, W., Tsirtsis, G., Lim, B., Krishnan, S., and F. Dupont, "Mobile IPv6 Residual Threats", draft-haddad-mext-mip6-residual-threats-02 (work in progress), July 2008.

[draft-ietf-mext-rfc3775bis] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", draft-ietf-mext-rfc3775bis-03 (work in progress), March 2009.

[draft-krishnan-mext-hld] Krishnan, S. and G. Tsirtsis, "MIPv6 Home Link Detection", draft-krishnan-mext-hld-01 (work in progress), March 2008.

Appendix A. MIPv6 Home Return

To keep the core of the document readable but still have the details available, this appendix provides a comprehensive analysis of MIPv6 main reference documents for what is related to Home Link detection and the ``Returning Home'' events.

A.1. Mobile IPv6 Home Link detection mechanism

The Mobile IPv6 Home Link detection mechanism is quite simple. In fact, it is specified in [RFC3775] by a simple sentence, in section 11.5.4 (``Returning Home''):

A mobile node detects that it has returned to its home link through the movement detection algorithm in use (Section 11.5.1), when the mobile node detects that its home subnet prefix is again on-link.

At the time of writing, MIPv6 specification is being revised and that part of the document has been enhanced, to support interactions with IKEv2 for Home Prefix Assignment [RFC5026]. Current version (02) of the draft [draft-ietf-mext-rfc3775bis] now includes a new specific subsection providing a simple detection algorithm (based on [draft-krishnan-mext-hld]) . The relevant part of the algorithm is provided below:

...

- Given the availability of the home prefix, the MN checks whether or not the home prefix matches one of the prefixes received in the RA. If it does, the MN concludes that it has returned home.

...

It basically goes in the same direction as [RFC3775]: Mobile Node considers itself on its home link if it detects a match between an advertised prefix and its home subnet prefix.

In the end, the expected Home Link detection mechanism has not been modified compared to the one specified in the original MIPv6 specification: simply put, if the MN finds itself on a link where its Home Subnet Prefix is advertised, it considers itself at home.

A.2. Emission of deregistration BU by the MN

This excerpt from section 11.5.4 (``Returning Home'') of [RFC3776] (In current revision 02 of the document [draft-ietf-mext-rfc3775bis], the section has not been modified, but now has number 11.5.5) describes the emission of the deregistration BU to the HA, just after

it has detected it is at home (using previous mechanism):

...

The mobile node SHOULD then send a Binding Update to its home agent, to instruct its home agent to no longer intercept or tunnel packets for it. In this home registration, the mobile node MUST set the Acknowledge (A) and Home Registration (H) bits, set the Lifetime field to zero, and set the care-of address for the binding to the mobile node's own home address. The mobile node MUST use its home address as the source address in the Binding Update.

...

As for all Binding Update messages sent to the Home Agent as part of Home Registration, IPsec protection is expected. Usually, in order for the CoA information to be IPsec protected (ESP does not provide protection for packet source address), the Alternate CoA Option must be present in the BU. This is explicitly stated in Section 11.7.1 (``Sending Binding Updates to the Home Agent'') of [RFC3776]:

...

o The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Update. This option MUST be included in all home registrations, as the ESP protocol will not be able to protect care-of addresses in the IPv6 header. (Mobile IPv6 implementations that know they are using IPsec AH to protect a particular message might avoid this option. For brevity the usage of AH is not discussed in this document.)

...

Nonetheless, this expected behavior is somewhat different when the Mobile Node is at home and needs to send its Binding Update. This is

described at the end of the following excerpt from Section 4.3 (``IPsec Protocol Processing'') of [RFC3776]:

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.

More specifically, as described in section 11.5.4 of [RFC3775], the HoA must be set as source address of the Binding Update message:

...

In this home registration, the mobile node MUST set [...] the care-of address for the binding to the mobile node's own home address. The mobile node MUST use its home address as the source address in the Binding Update.

...

Still in [RFC3776] (Section 3.1,``Binding Updates and Acknowledgements''), specific examples of expected packet layouts are given for registration when the node comes back home:

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
```

This layout is associated with ``MUST support'' statements and is expected to be used. Note that [RFC4877], the revised version of [RFC3776], provides the same description and expects the same behavior.

It is interesting to note that MIPv6 specification splits the

emission and validation steps: previous discussion were associated with the emission of the deregistration BU by the MN. Processing rules for validation and parsing of BU by the HA when receiving it are covered in different sections of the document and discussed later in next subsection.

A.3. Receipt and validation of deregistration BU by the HA

The reference documents require that Home Agent supports previous Layout for deregistration Binding Update. Even if this is probably the expected layout, this is not the only possible solution. Additional information are given in Section 9.5.1 of [RFC3775], for validating Binding Update messages in general.

Section 10.3.2 of [RFC3775] covers in details ``Primary Care-of Address De-Registration''. Here, the validation of deregistration BU format by the HA leaves room for different layouts:

A binding may need to be de-registered when the mobile node returns home or when the mobile node knows that it will not have any
  care-of addresses in the visited network.

A Binding Update is validated and authorized in the manner described in the previous section; note that when the mobile node de-registers when it is at home, it may not include the Home Address destination option, in which case the mobile node's home address is the source IP address of the de-registration Binding Update. This section describes the processing of a valid Binding Update that requests the receiving node to no longer serve as its home agent, de-registering its primary care-of address.

The non-normative ``may not include the Home Address destination option'' is ambiguous and error-prone: section 11.5.4 has a ``MUST use its home address as the source address in the Binding Update''. If the Home Agent allows deregistration BUs with Home Address destination option, this leaves room for those to be sent from a foreign network, probably to support the case where ``the mobile node knows that it will not have any care-of addresses in the visited network''.

Because of the rules for determining care-of address and home address, provided in section 9.5.1

The specified care-of address MUST be determined as follows:

- If the Alternate Care-of Address option is present, the care-of address is the address in that option.
- Otherwise, the care-of address is the Source Address field in the packet's IPv6 header.

The home address for the binding MUST be determined as follows:

- If the Home Address destination option is present, the home address is the address in that option.

o Otherwise, the home address is the Source Address field in the packet's IPv6 header.

The following various deregistration BU sent by a Mobile Node should probably be considered valid (even if the specific layout may not be supported on a specific implementation):

```
IPv6 header (source = some address (possibly the HoA),
             destination = home agent)
ESP header in transport mode
Mobility header
   Binding Update
      Alternate Care-of Address option (Home Address)
```

```
IPv6 header (source = Home Address,
             destination = home agent)
Destination Options header
   Home Address option (home address)
ESP header in transport mode
Mobility header
   Binding Update
```

```
IPv6 header (source = some address (possibly the HoA),
             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 (Home Address)
```

The last example is the common layout expected by the HA when the MN

is on a foreign network.

The point here is that the expected layout for deregistration BU sent by the MN should be strictly checked by the HA when receiving the BU. It seems that the receiving rules for the HA are not that strict, possibly to support the case where ``mobile node knows that it will not have any care-of addresses in the visited network''.

A.4. Local impacts of BU processing on the HA and emission of BA

In this subsection, we just make the hypothesis that the HA has received a deregistration BU which it has considered valid and that it has determined the care-of address and the home-address as described in section 9.5.1 of [RFC3775], quoted in previous subsection.

The expected behavior by the HA is to remove the binding (local modification of MIPv6 related structures). It is also expected (even if not mandatory) that the tunnel with the Mobile Node be removed, now that it is back home. This is described at the end of section 11.5.4 of [RFC3775]:

Note that the tunnel via the home agent typically stops operating at the same time that the home registration is deleted.

When IPsec is used for protecting tunneled traffic, the same behavior is expected. Section 4.2 of [RFC4877] specifies that:

- 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, SHOULD 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, Binding Acknowledgements and Mobile Prefix Discovery messages SHOULD NOT be deleted as they do not depend on care-of addresses and can be used again.

This SHOULD in [RFC4877] was a MUST in [RFC3776]. The protection of BU/BA traffic using ESP in transport mode is unmodified by the deregistration.

After those changes, the HA sends back a BA to the MN. This is required because the A bit is set in the BU sent by the MN for de-registration, a BA is always sent by the HA, as described in section 9.5.4 of [draft-ietf-mext-rfc3775bis]:

- If the Binding Update was discarded as described in Section 9.2 or Section 9.5.1, a Binding Acknowledgement MUST NOT be sent. Otherwise the treatment depends on the following rules.

- If the Acknowledge (A) bit set is set in the Binding Update, a Binding Acknowledgement MUST be sent. Otherwise, the treatment depends on the below rule.

- If the node rejects the Binding Update due to an expired nonce index, sequence number being out of window (Section 9.5.1), or insufficiency of resources (Section 9.5.2), a Binding Acknowledgement MUST be sent. If the node accepts the Binding Update, the Binding Acknowledgement SHOULD NOT be sent.

This means that following the emission of a deregistration BU, a MN should expect to receive a BA.

With regard to the address the BA is sent, section 9.5.4 of [RFC3775] contains the following:

If the Source Address field of the IPv6 header that carried the Binding Update does not contain a unicast address, the Binding Acknowledgement MUST NOT be sent and the Binding Update packet MUST be silently discarded. Otherwise, the acknowledgement MUST be sent to the Source Address. Unlike the treatment of regular packets, this addressing procedure does not use information from the Binding Cache.

However, a routing header is needed in some cases. If the Source Address is the home address of the mobile node, i.e., the Binding Update did not contain a Home Address destination option, then the Binding Acknowledgement MUST be sent to that address and the routing header MUST NOT be used. Otherwise, the Binding Acknowledgement MUST be sent using a type 2 routing header which contains the mobile node's home address.

This basically implies that a deregistration BU with a HAO will possibly trigger a BA with a RH2 sent to whatever address was in the IPv6 header source address field in the BU. Simply put, the BA is expect to be sent to the real address from which the BU was sent.

In section 3.1 of [RFC3776], the common cases for the deregistration BA sent from the home network is covered:

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
```

A.5. Local impact associated with BU emission and BA processing on the MN

Once it has sent the deregistration BU, the MN is expected to perform some modification of its ND behavior, as discussed in section 11.5.5 (``Returning home'') of [draft-ietf-mext-rfc3775bis]. Some final changes are performed after receiving the BA from the HA:

After the Mobile Node sends the Binding Update, it MUST be prepared to reply to Neighbor Solicitations for its home address. Such replies MUST be sent using a unicast Neighbor Advertisement to the sender's link-layer address. It is necessary to reply, since sending the Binding Acknowledgement from the home agent may require performing Neighbor Discovery, and the mobile node may not be able to distinguish Neighbor Solicitations coming from the home agent from other Neighbor Solicitations. Note that a race condition exists where both the mobile node and the home agent respond to the same solicitations sent by other nodes; this will be only temporary, however, until the Binding Update is accepted.

After receiving the Binding Acknowledgement for its Binding Update to its home agent, the mobile node MUST multicast onto the home link (to the all-nodes multicast address) a Neighbor Advertisement [20], to advertise the mobile node's own link-layer address for its own home address.

The specification focuses on link layer interactions but does not provide information on the timing associated with the removal of the tunnel and/or IPsec Security Policies for tunnel traffic. For performance reasons it usually happens when the BU is sent (UMIP, the linux implementation, does just that) to avoid sending packets with a possibly invalid source address (the old CoA) while waiting for the BA to come back.

If the same timing is kept when returning home, the MN will drop its IPsec protection as soon as it has sent the deregistration Binding Update.

Appendix B. Acknowledgements

The author acknowledges the comments and corrections provided by Jean-Michel Combes, Tony Cheneau, Nicolas Bareil and Romain Kuntz on an initial version of the document.

The work on this document was done in the context of MobiSEND project, partially funded by the french "National Research Agency (ANR)".

This document was generated by xml2rfc.

Author's Address

Arnaud Ebalard
EADS Innovation Works
12, rue Pasteur - BP76
Suresnes 92152
France

Phone: +33 1 46 97 30 28
Email: arnaud.ebalard@eads.net