Network Working Group	A. Ebalard	
Internet-Draft	EADS	
Intended status: Informational	May 21, 2009	
Expires: November 22, 2009		

TOC

Mobile IPv6 IPsec Route Optimization (IRO)
draft-ebalard-mext-ipsec-ro-01

Status of this Memo

Copyright Notice

Abstract

This memo specifies an improved alternate route optimization procedure for Mobile IPv6 designed specifically for environments where IPsec is used between peers (most probably with IKE). The replacement of the complex Return Routability procedure for a simple mechanism and the removal of HAO and RH2 extensions from exchanged packets result in performance and security improvements.

Table of Contents

---

1. Disclaimer and conventions

TOC

TOC

1.1. Disclaimer

This memo covers MIPv6 Route Optimization in IPsec/IKE environments. For that reasons it is expected that the reader be familiar with the main reference documents associated with those topics.
This includes the main MIPv6 reference documents ([RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.), [RFC3776] (Arkko, J., Devarapalli, V., and F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents,” June 2004.), [RFC4877] (Devarapalli, V., “Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture,” April 2007.), ...) and main IPsec/IKE reference documents ([RFC4301] (Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” December 2005.), [RFC4303] (Kent, S., “IP Encapsulating Security Payload (ESP),” December 2005.), [RFC4306] (Kaufman, C., “Internet Key Exchange (IKEv2) Protocol,” December 2005.) and their previous versions).
For the discussions regarding the security of route optimization (proof of address ownership, mainly) [RFC4225] (Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, “Mobile IP Version 6 Route Optimization Security Design Background,” December 2005.) is a must read and [RFC4651] (Vogt, C. and J. Arkko, “A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization,” February 2007.) provides a good summary of the issues and previous work on possible solutions.
The Security Considerations section (section 6) of [RFC4866] (Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” May 2007.) also provides a good security-oriented introduction to the address ownership problem.

1.2. Conventions used in this document

TOC

In this document, except otherwise specified:

- "IKE" is used as a placeholder for both IKEv1 (Harkins, D. and D. Carrel, “The Internet Key Exchange (IKE),” November 1998.) [RFC2409] and IKEv2 (Kaufman, C., “Internet Key Exchange (IKEv2) Protocol,” December 2005.) [RFC4306].

- "Peer" is used as a placeholder for a MIPv6 end entity, i.e. a CN or a MN.

- "HAO" is used as a placeholder for Destination Options Header carrying a Home Address Option. When the address in a HAO is considered, it denotes the address found in the Home Address field of the Home Address option carried in the Destination Options Header.

*When "tunnel" is used to designate the IPv6-in-IPv6 path between the MN and its HA, IPsec in tunnel mode is assumed to be in place.

*When "MN-CN" is used it also obviously includes the MN-MN case where the second MN acts as a CN for the first MN.

*When "IPsec flow" applies to a MN-MN or MN-CN communication, the address of the MN considered for the associated SP is the HoA.

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] (Bradner, S., ""Key Words for Use in RFCs to Indicate Requirement Levels"," March 1997.).

---

2. Introduction

TOC

2.1. Current situation

TOC

Mobile IPv6 specification (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.) [RFC3775] mandates the use of IPsec for protection of communications (control and optionally data) between a Mobile Node and its Home Agent. Support for static keying is made mandatory, and dynamic keying optional. The protection is made possible by the trust relationship that preexists between the HA and the MN: they belong to a common trust domain (the same network, a PKI). Interactions between MIPv6 and IPsec/IKE for MN and HA exchanges are partly covered in [RFC3776] (Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents," June 2004.) and [RFC4877] (Devarapalli, V., "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture," April 2007.). For implementation reasons outside the scope of previous reference documents, some additional changes to IPsec/IKE are required to support Mobile IPv6. [MIGRATE] (Ebalard, A. and S. Decugis, "PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE," August 2008.) specifies a way to implement those changes by extending PF_KEY framework.
[RFC3775] (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.) also specifies a Route Optimization procedure which allows direct communications to occur between a Mobile Node (MN) and a Correspondent Node (CN), without suffering the delay associated with the routing through the MN's Home Agent. The setup of this optimized

routing is based on a mechanism called Return Routability Procedure (RRP).
One of the main hypothesis behind the design of Return Routability Procedure is the lack of trust relationship between the MN and its CN. This results in a complete lack of security in terms of privacy and authentication of data: the procedure mainly provides a limited proof of MN's HoA and CoA addresses ownership to the CN.
In trust domains (networks with an underlying PKI infrastructure) where Mobile IPv6 gets deployed using dynamic keying (IKE or IKEv2) for negotiating Security Associations, Mobile Nodes are already provisioned with credentials (X.509 certificates). In those environments, the initial hypothesis that led to the design of RRP and its associated limited security abilities does not hold anymore.
At the moment, [CNIPsec] (Dupont, F. and JM. Combes, “Using IPsec between Mobile and Correspondent IPv6 Nodes,” August 2008.) only describes how IPsec can be used to protect signaling traffic between the Mobile Node and the Correspondent Node but only provides a limited coverage of the problem.

2.2. Characteristics of IRO

TOC

This document defines an extension of Mobile IPv6 protocol that aims at replacing common RRP and RO procedures by a mechanism called IPsec Route Optimization (IRO) in environments where IPsec and IKE are used. It allows MN to mount and maintain direct IPsec-protected communications with CN and other MN with which they share some trust relationship, in a completely transparent fashion for upper layer protocols.
IRO is not a detailed set of requirements for IPsec to work between MN and CN but a new mechanism resulting from the tight integration and joint efforts of MIPv6, IKE and IPsec to provide a secure and scalable mobility service.
The main functional and security advantages that best describe IRO are:

- Protected MN-CN binding using IKE-negotiated IPsec SAs.
- Complete transparency for IKE (negotiation, rekeying, movement, ...) and other upper layers, including layer 14 (the user).
- Compatibility with both tunnel and transport mode IPsec protection between peers.
- Compatibility with static keying (See Appendix G (Compatibility with static keying)).
- In MN-CN case, non-disclosure of MN's HoA on its foreign link.

*No additional changes to IPsec or IKE protocols and limited changes to MIPv6 via four simple messages and an option resulting in simple and generic integration within IPsec and Mobile IPv6 stacks.

*Improved and more generic proof of address ownership mechanism.

*Safe by default behavior avoiding direct unprotected traffic flows.

*Complete removal of RH2 and HAO, resulting in simplified packet handling on both sides and possibly better compatibility with filtering implemented in the network.

*Per packet MTU gains between 24 and 48 bytes in comparison with equivalent uses of IPsec in standard RO context. Details are provided in Appendix F (MTU Gains).

The main prerequisites of IRO are:

*Existence of a trust relationship between peers (i.e. shared secret or ability to use IKE).

*Required protection of peers' exchanges (i.e. IPsec is used between peers). IRO does not apply to direct unprotected communications between peers. More precisely, IRO prevents them.

*To fully benefit from IRO improvements, data traffic between the MN and its HA must be exchanged through an IKE-negotiated movement resistant IPsec tunnel. If this hypothesis is not fulfilled, IRO will still be usable but some security features listed previously will be lost (Appendix D (Lack of encryption between MN and HA)).

2.3. Motivation

TOC

The motivation behind this work is the direct need for both efficient and secure communications in Mobile IPv6 environments already benefiting from an underlying trust domain.
The first intended target of the mechanism described in this memo is the growing number of corporate networks where PKI are now widespread. This is generally due to the increasing number of services (802.1X, SSL/IPsec VPN, TLS Web portal, S/MIME, ...) that use them on a daily basis as the root of their security and to provide logical segregation. It is also suitable for other kinds of communities.

In environments where data confidentiality and privacy do matter (IPsec is used for the protection of data between the MN and its HA), current RRP and RO between peers of the trust domain are usually deactivated:

- to prevent direct unprotected communications between peers that would bypass protected tunneling through the Home Network.

- because their implementation and setup with IPsec/IKE does not work out of the box and is not trivial even if [CNIPsec] (Dupont, F. and JM. Combes, "Using IPsec between Mobile and Correspondent IPv6 Nodes," August 2008.) helps for signaling.

This results in heavy constraints on the HA (which handles all the traffic to/from its MN) and the de-facto inability to get direct end-to-end IPsec-protected MN-CN and MN-MN communications.
The ability to reduce the number of communications performed by the Mobile Node that get tunneled through the HA is both an improvement in term of upload bandwidth consumption on the link to the HA, cryptographic processing requirements on the HA and also in term of latency for applications that directly benefit from end-to-end connections, like Chat, VoIP, Videoconferencing or direct file exchanges.
In a sense, there is a kind of vicious circle regarding the use of IPsec/IKE with various protocols, including MIPv6: because dynamic keying and IPsec are not considered the common case, they are not fully covered in specifications (static keying for simple modes). The net effect is that their implementation and deployment is then complicated, which results in limited use. In a sense, IRO tries to break that circle. Simply put, this specification considers IKE-enabled environments as the first target and then covers static keying cases.

2.4. Notes to the reader

TOC

The mechanism described in this memo is very simple from a design perspective. To keep this apparent simplicity and the reading of the document pleasant, all design decisions and main justifications are provided in the numerous appendices (around 10 pages). This allows to focus on the details of the mechanism in the body of the document (around 20 pages).
For previous reason, the reading of the document can be performed linearly. The not so curious reader can skip over the appendices which are only a must read for developers and security people to acquire a deep understanding of the mechanism and how security has been taken into account in its design.
Unlike many other IETF documents, this memo voluntarily provides a practical implementation feedback geared towards developers. Even if

the associated section does not mandate an implementation design, it might be of interest anyway.

---

3. Overview

TOC

The whole document is geared towards improved security between MIPv6 nodes and also improved usability of IPsec/IKE with MIPv6. This section provides to the reader a quick non-normative overview of how IRO works, before entering the details of the mechanism in next sections. The reader is expected to be familiar with the vocabulary used in [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.). We do not consider in this section the relationship between the MN and its HA, only the relationship between a MN and its CNs. In the whole document, IKE is considered as the default mechanism used for SA setup.
This section provides a quick and non-normative overview of IRO and introduces next sections that contain normative details. The first subsection provides a rough outline of IRO. It is followed by 5 small subsections that cover the steps of IRO processing, in the order they occur:

* Pre-binding steps: installation of remapping rules, which IRO uses to prevent the use of RH2 and HAO in incoming and outgoing signaling packets (MH traffic).

* BU emission: description of the steps that apply to the emission of the BU by the MN in the context of IRO.

* Proof of CoA ownership: description of the steps that occur when a proof of CoA ownership is requested by the peer.

* BA emission: description of the steps that apply to the emission of the BA to the MN in the context of IRO.

* Post-binding steps: installation of additional remapping rules, which IRO uses to prevent the use of RH2 and HAO in incoming and outgoing data packets.

3.1. The big picture

TOC

This section simply lists the key ideas and design concepts behind IRO.

When IPsec is used between two peers, every packet de facto contains a simple piece of information (the SPI) that gives access to many parameters. Among those parameters synchronized between the two IPsec stacks are address information for both peers. Unlike IPsec, MIPv6 uses specific extensions (RH2 and HAO) to explicitly carry address information. When both protocols are used together and the IPsec SA/SP make use of HoA (i.e. not CoA), the RH2 and HAO extensions in packets carry the HoA. It could easily be deduced from the SPI. Based on this observation, IRO removes RH2 and HAO extensions from packets and replace them by simple additional steps on the sender and the receiver: remapping rules for address based on the SPI.
Previous removal of HAO and RH2 extensions from traffic between peers is also perfectly applicable to the traffic between a MN and its HA. This specification extend the remapping rules to the traffic between a MN and its HA. When IRO is used, RH2 and HAO extensions are simply not seen on the wire.
As stated previously, the hypothesis on which common RO and RRP are based simply do not hold when peers are able to use IPsec/IKE between them. For that reason, even if some proof of address ownership is still required, a more suitable (read simple) mechanism is defined for that purpose.
To sum it up (simplistic vision):

*IRO simplifies packets format by removing HAO and RH2 extensions.

*IRO fully replaces RRP by a more suitable and simple mechanism taking into account the use of IPsec/IKE between peers.

*IRO defines how this can be extended to MN-HA exchanges.

3.2. Pre-binding steps

TOC

Before any direct communication can take place between a MN and a CN, the CN must accept a binding between the CoA and the HoA of the MN. For that to happen, the CN must have acquired the proof of both HoA and CoA addresses ownership by the MN.
In RRP, the MN proves to the CN its ability to both send and receive traffic from and at those addresses by a four messages exchange combining both direct and HA-tunneled packets.
In the context of IRO, the binding registration between peers is IPsec protected. It is expected that IKE be used for negotiating an initial pair of ESP transport mode IPsec SAs between the HoA of the MN and the address of the CN for protecting this registration (static keying is covered later in the document). IKE negotiation occurs using the tunnel

between the MN and its HA, i.e. the MN uses the HoA for that purpose. This provides the CN the initial proof of HoA ownership by the MN.
On both entities, the specific IPsec ESP transport mode SAs (protecting MH traffic) created between the peers are taken into account by IRO code in Mobile IPv6 stack. This triggers the setup of specific "remapping rules" on both entities, that will be applied to incoming and outgoing IPsec packets whose SPI matches the one of tracked SAs:

1. On the MN, the outgoing IPsec traffic matching the SPI of the associated SA to the CN has its source address remapped to the address stored (by MIPv6 process) in the ancillary data of the packet (the CoA).

2. On the CN, the incoming IPsec traffic matching the SPI of the associated SA with the MN has its source address remapped to the specific source address in the SA (the HoA of the MN). The remapped address is kept as an ancillary data in the local packet structure for further processing. The packet is then naturally handled by the IPsec stack.

3. On the CN, the outgoing IPsec traffic matching the SPI of the associated SA to the MN has its destination address remapped to the address stored in the ancillary data of the packet, if not null.

4. On the MN, the incoming IPsec traffic matching the SPI of the associated SA to the CN has its destination address compared with the CoA the MN is asking a binding for to the CN. On match, the destination address of the IPsec packet is remapped to the destination address in the SA (the HoA of the MN). The packet is then naturally handled by the IPsec stack.

Simply stated, rules 1 and 3 will end up performing a remapping of HoA used in outgoing IPsec packets in their CoA counterparts and rules 2 and 4 will do the opposite on the other side for incoming IPsec packets.
Note that these rules apply only to IPsec packets associated with SA that protect MH traffic. They are used before any data packet is received or sent by the entities using a direct path.

3.3. BU emission

TOC

The MIPv6 stack on the MN emits a Binding Update packet containing a Mobility Header AltCoA option which carries the CoA it is proposing a binding for to the CN. This packet is sent from the HoA of the MN to the address of the peer. The CoA is put as an ancillary data in the

local packet structure for further processing. As it matches the IPsec SA put in place between the MN and the peer, it gets handled by the IPsec stack to be ESP protected. Before leaving the MN, it passes the set of MIPv6 rules for the MN; a match is found against rule 1, so that the source address of the packet is remapped to the address available as an ancillary data in the packet, the CoA of the MN.
When the IPsec protected BU hits the MN, it passes the set of MIPv6 rules for the CN. It matches rule 2 so that its source address is remapped to the source address of the SA (the HoA of the MN). The source address found in the packet is stored as ancillary data. The packet is handled by the IPsec module, matches the SA, is decrypted and passed to the upper layer, the MIPv6 process.
During parsing, the CN compares the content of the AltCoA option with the address previously stored as ancillary data.

3.4. Proof of CoA ownership

TOC

At that point, before accepting the binding and replying with a BA, the CN must have the proof of CoA ownership from the MN. If one is already available, it simply goes on and sends a BA, as described in 3.4. Otherwise, it first performs following steps.
It sends a newly defined MH message (AOTC, Address Ownership Test Challenge) to the MN, providing the CoA as ancillary data, so that the remapping rules will make the packet use the CoA for the address found in the IPv6 header destination field. This packets carries a freshly generated nonce.
On the MN, the packet follows the reverse remapping process, the CoA being remapped to the HoA and passed as ancillary data. The MIPv6 stack replies with an IPsec protected MH message to the CN (AOTR, Address Ownership Test Request), using the HoA as local source but providing the CoA as ancillary data. The remapping rule makes the CoA the on-wire address of the packet. This packets carries the nonce sent by the CN.
The CN receives the packet and after having checked the source address and the nonce against the one previously sent, the MIPv6 stack records the address ownership of the CoA for that MN, and continues with the steps described in Section 3.5 (BA emission)

3.5. BA emission

TOC

The CN constructs a Binding Acknowledgement packet to be sent to the HoA of the MN. The CoA of the MN is put as an ancillary data in the local packet structure for further processing. Now, as the BA matches the SA, it is ESP-protected and passes the set of MIPv6 rules for the CN. It matches rule 3 and the HoA is replaced with the address

available in the ancillary data of the packet (MN's CoA). The packet is then sent. At that moment, if the status code in the BA is 0 (Binding Update Accepted), the binding is effective on the CN.
On the MN, the IPsec protected BA is received, it passes through the set of MIPv6 rules for the MN and matches rule 4. The destination address is changed to the destination address of the SA (HoA of the MN). It is then handled by the IPsec module, and then to the MIPv6 process. If the status code in the BA is 0, the binding is effective on the MN.
For the rest of this section, we consider the binding is effective on both sides. Other scenarios are covered in details in Section 3 (Overview).

3.6. Post-bindings steps

TOC

In [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.), when the RRP has completed successfully, routing of traffic between the MN and the CN is automatically modified to follow a direct path. With IRO, on the contrary, a successful binding between a MN and a CN does not trigger any change in routing of _regular_ traffic between the MN and the CN. It still flows using the IPsec tunnel through the MN's HA. Only IPsec traffic is optimized.
This design decision provides a "safe by default" behavior and avoid a successful binding to lead to unprotected direct communications. Furthermore, only IPsec flows will be able to take advantage of the direct path between the MN and the CN. Arguments for this design are provided in Appendix E (What if I don't need protection?).
So, if existing IPsec SAs protecting non-signaling traffic (data) are already available on both sides, that have the HoA and the address of the MN as address selectors, remapping rules are put in place to perform the same kind of address changes presented in four previous rules. Those rules are static ones (they do not use any ancillary data) that remap CoA to HoA and HoA to CoA (after some checks), respectively before and after IPsec processing.
They simply replace the HAO and RH2 headers inclusion and parsing on both sides by using the SPI information as an opaque multiplexing/ demultiplexing value available on both ends.

---

4. Proof of CoA ownership

TOC

TOC

4.1. Position of the problem

A CN accepting a binding for the CoA of a peer is not something harmless. In the context of IRO, this decision is based on:

- a proof of HoA ownership by the MN at the time the SA is negotiated.
- a proof of CoA ownership by the MN.

The existence of a strong trust relationship between the two (pairs of SA) and an easy proof of emission capability from the CoA are unfortunately insufficient proofs of CoA ownership. As covered in Appendix A (Ability to send does not prove CoA ownership), a proof of the ability for the MN to receive traffic at its asserted CoA is required to workaround the lack of ingress-filtering at the scale of Internet: it avoids the CN to involuntarily take part in a DoS against the provided CoA.

4.2. Overview

TOC

As the proof of HoA ownership is only required to occur once in the context of IRO, the mechanism focuses on the proof of CoA ownership. Instead of reusing the complicated RRP, IRO directly benefits from the available IPsec protection between the MN and its CN to simplify things.
Furthermore, in the context of IRO, the lifetime of the provided proof is no longer limited and generally de-correlated from registration steps. This already reduces the amount of transferred data and leaves room for further optimizations (nodes with multiple simultaneous connections, nodes with limited numbers of foreign networks, ...)
As CoTI and CoT messages have some associated requirements, options and semantic, and also lacks some expressiveness, they are not reused for IRO proof of address ownership. It is based on four new extremely simple messages:

- AOTO: Sent by a MN to a CN to offer to prove address ownership.
- AOTC: Sent by a CN to the MN at the address to be tested, with a Nonce option that will be returned in an AOTR message.
- AOTR: Sent by the MN as a response to an AOTC, with the received Nonce option.

*AOTS: Sent by the CN to the MN to provide a status on ongoing address ownership test.

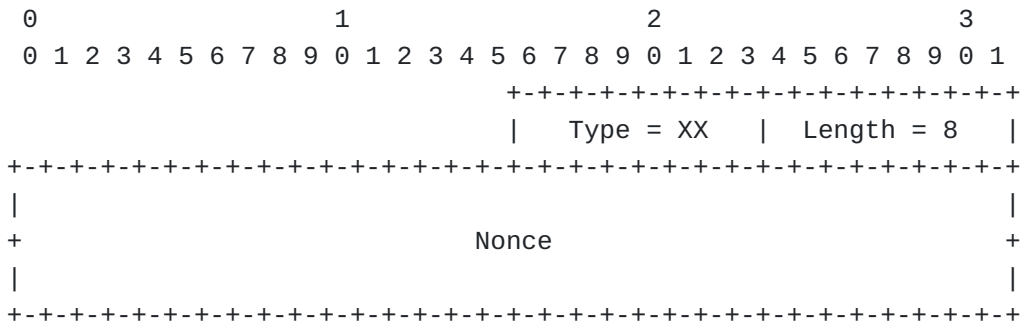
4.3. Mobility Options

TOC

4.3.1. Nonce option

TOC

The Nonce option has type XX and an alignment requirement of 8n+6. Its format is as follows:



The content of the Nonce field MUST always be filled with a freshly generated 64-bit random value.
XXX For testing purposes, the Nonce option has type value 88.

4.4. IRO Messages

TOC

All the normative information associated with the four new messages specified by IRO are provided in this subsection. This includes their format, associated constants, security related information and processing requirements.
Note that the messages defined below are used for proof of ownership of the CoA. They are not used to prove ownership of the HoA: this is either not done (static keying) or the result of the ability to negotiate SA using IKE.

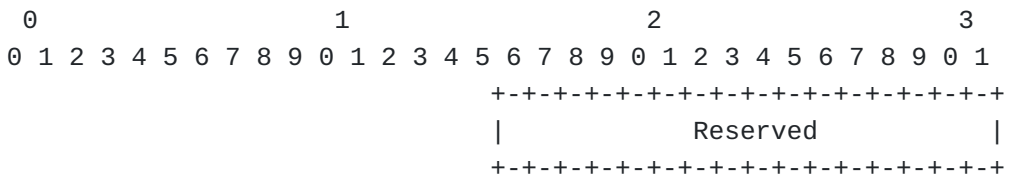
TOC

4.4.1. Address Ownership Test Offer (AOTO)

This message is sent by a MN to a CN to offer to prove its ownership of the CoA the packet was sent from. An AOTO message MUST NOT be sent by a MN if it is not already registered with the CN. If that happens, the CN simply drops the message without further processing. Reception of this message can trigger the emission of either:

- an AOTC containing a Nonce option, sent back to the source address of the AOTO.
- an AOTS with status 0, indicating that the peer does not allow the peer to pre-register CoA ownership information.
- an AOTS with status 1, indicating to the peer that the proof of Address ownership is still valid.
- nothing if it is invalid or sent by an unregistered MN.

The format of the message is as follows:



Reserved field is not used yet but might be for future need. It currently serves padding requirements. It should be set to null on emission and ignored on reception by peers complying with this specification.
AOTO messages do not carry options. MH Type field in Mobility Header takes value XX when carrying an AOTO message.
XXX For test purposes, MH Type field should use value 30

4.4.2. Address Ownership Test Challenge (AOTC)

TOC

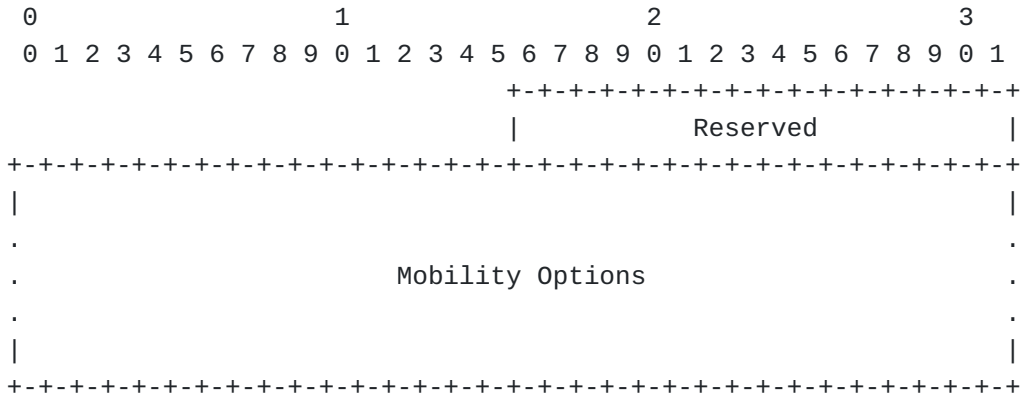
The purpose of this message is to provide a nonce to an MN at the address the MN wants to provide proof of ownership for. The ability for the MN to return the nonce to the CN (in an AOTR) provides a live proof of its ability to receive traffic at that address. This message is possibly sent by a CN to a MN in two situations:

- After receiving a Binding Update message that the CN is willing to accept but for which it does not already has a proof of

address ownership for the originating CoA the packet was sent from (correlated with the content of the AltCoA option).

*After receiving an AOTO from a MN that wants to perform a proof of address ownership for the source address of the packet.

The format of the message is as follows:



The Mobility Options field must always contain a Nonce option. The nonce must be stored locally by the CN for that MN, along with the address being tested. The nonce will be compared with the content of the nonce option found in the AOTR messages.
MH Type field in Mobility Header takes value XX when carrying an AOTC message.
XXX For test purposes, MH Type field should be set to 31

4.4.3. Address Ownership Test Response (AOTR)

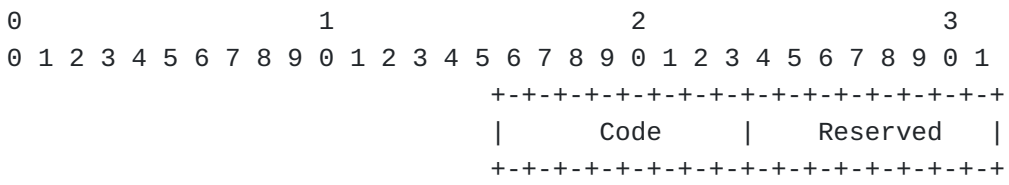
TOC

This message is sent by the MN as a result of receiving an AOTC (resulting from an initial action, BU or AOTO). It contains the same nonce, in a Nonce option, the peer had included in its AOTC. The AOTR message is sent from the address to be tested (the on-wire destination address of the AOTC).
When received by the CN, on-wire source address is used to access the stored nonce previously sent in an AOTC message and compare it with the one in the Nonce option found in the message. On match, the address ownership by the peer is considered proved.
The format of the message is the same as the AOTC message except for MH Type field in Mobility Header which takes value XX when carrying an AOTR message.
XXX For test purposes, MH Type field should be set to 32

TOC

4.4.4. Address Ownership Test Status (AOTS)

This message is sent by the CN with a status regarding a proof of address ownership. The status can be generic (not associated to an address whose ownership is being proved), for instance if this CN does not allow MN initiated Address Ownership Tests to occur. It can also be specific to an ongoing or already performed Test of Address Ownership, for instance to explicitly acknowledge the result of the test.



MH Type field in Mobility Header takes value XX when carrying an AOTS message. Code field provides the status code the message carries. The list of status codes is provided below:
AOTS status codes:

*0 AOTO not allowed

*1 Proof of Address Ownership is valid

XXX For test purposes, MH Type field should be set to value 33

4.5. Concrete uses of AOT* Messages

TOC

4.5.1. Registration with a CN

TOC

The registration process between a MN and its HA is simple and efficient, being made of a simple BU [/BA] exchange. This is because the proof of CoA ownership is not required by the HA from the MN.
Like with other route optimization procedures, with IRO, the CN is required to have a proof of CoA ownership available for the MN before accepting a binding and replying with a Binding Ack. More precisely, the proof is needed only before sending traffic to the CoA of the MN but does not impact the reception of traffic from the CoA. This is of particular importance in the rest of the discussion.
Unlike in other more common environments where the proof has to be made at every binding, or "renewed", IRO uses proofs with unlimited lifetimes. This does not mean that once the ownership has been proved

to a CN the CoA will indefinitely belong to a MN. The decision is always left to the CN, with the expectation that some sufficient temporary storage will make it capable to keep the binding for a while. This means that if a proof of CoA ownership for a MN is available locally on its CN, no live proof is required and a simple BU [/BA] exchange is sufficient for the registration to occur. This also means that inside small or medium communities, where MN move between few locations, the number of potential CoA remains quite low and stable, and can be kept locally on nodes acting as CN.
For instance, without limiting the possible uses, a typical scenario for a daily use includes an address at home (wifi, ...), another on a mobile network (3G, ...) and another at work (wifi, Ethernet, ...).
With IRO, when a MN sends a BU to a CN for registration or reregistration purposes, it starts directing its traffic instantly after the emission of the BU to the address of the CN. Then, the CN will either ask for proof of CoA ownership if it has none available from that MN for that CoA or send a BA to the peer. In all cases, it puts in place the remapping rules for accepting traffic from the CoA (and not the one for emission). That way, there is no disruption of traffic from the MN to the CN.
If the CN replies with an AOTC message sent to the CoA of the MN, the MN replies with an AOTR, proving its complete ownership. The CN then replies with the expected BA and puts in place the required remapping rules for the traffic to flow to the MN at its CoA.
Regarding re-emission, if the MN has no reply from the CN (i.e. no BA or AOTC), common re-emission rules apply. Then, if the CN has sent an AOTC, but receives no reply, it can keep things that way or garbage collect the remapping rule (i.e. remove it after some time). If the MN receives no BA from the CN, it performs re-emission of the AOTR (This implies that the Nonce must be kept locally on the CN even after the emission of the BA).

4.5.2. Early test of CoA ownership

TOC

There are cases where a MN will be willing to perform early proof of address ownership, allowing it to avoid the delay during movement. In that case, the MN sends an AOTO message to the CN, and receives either and AOTC or an AOTS. If the received message is an AOTS, the exchange is over. If the message is an AOTC, it replies with an AOTR and waits for an AOTS.
A possible use of that early test of CoA ownership is by multi-homed nodes that already have a list of possible CoAs they will switch to if they lose their primary connectivity mean. Note that:

this is only a possible optimization allowed by the AOT framework introduced in this document, not a requirement.

*it still requires the MN to be registered with the CN.

it requires the MN to exchange AOT messages using the address whose ownership is to be proved.

4.5.3. Test of HoA ownership

TOC

IRO does not mandate regular proofs of HoA ownership, for the reasons covered in Appendix C (Arguments for no regular check of HoA ownership). For those who have the need, and can afford to lose the associated bits on a regular basis, the AOT* messages can be used for that purpose.
If a CN wants to get a live proof of HoA ownership from a MN, it simply emits an AOTC message (with a fresh Nonce option) to the HoA of the MN for which it has already accepted a registration. The MN MUST reply with an AOTR message containing the received Nonce option. The exchange occurs using respectively the HoA as on-wire destination and source address. This implies that the packets are tunneled through MN's HA. In the MN-MN case, this mainly results in packets never following a direct path.
Note that this specification does not define the action taken by a CN if it does not receive AOTR messages as response to its AOTC messages sent to the HoA.

---

5. Remapping rules

TOC

This section covers the heart of IRO processing, the remapping rules that are applied to incoming and outgoing IPsec protected traffic.

5.1. Requirements

TOC

TOC

5.1.1. On-wire addresses access from userland

With IRO, there is a need for the MIPv6 processing engine to both pass and get on-wire source and destination addresses of received and emitted IPsec protected MH packets. This need is mainly associated with the proof of address ownership and binding exchanges. The need is simply the same as the one associated with the ability to set and get HAO/RH2 for a common MIPv6 process. Instead of having explicit information in the packet, an ancillary path is required.
This requirement is limited only to MH traffic in general and some specific MH types in particular.
For incoming IPsec protected MH packets, this means that during the handling by remapping rules, the remapped on-wire address must be kept in the local packet structure as an ancillary data that the MIPv6 process will be able to access.
For outgoing MH packets, this means that the addresses MUST be made available as ancillary data in the local packet structures by the MIPv6 process and then be used, if available, by the remapping rules.
For all incoming IPsec packets associated with a coarse or fine grained SA for MH traffic, if a remapping rule is applied to the traffic, the on-wire source and destination addresses MUST be made available as ancillary data to the userland process that will process the packet (i.e. at socket level). In all cases (remapping rule being applied or not), if an on-wire source or destination address is not changed, the associated ancillary data MUST contain the unspecified address (::).

5.1.2. Non-MH traffic (data traffic) TOC

Data traffic exchanged between MN and CN using IRO has simple requirements in term of remapping. We consider here only IPsec packets that are not associated with a transport mode IPsec SA protecting MH traffic.

5.1.2.1. Compatibility with traffic using RH2 and HAO TOC

This specification is compatible with RH2 and HAO extensions even if some care is obviously required in the order in which they are handled. This is generally an implementation dependent issue outside the scope of this specification.
In practice, it is expected (except otherwise specified) that IRO module handles incoming traffic after RH* or HAO processing and outgoing traffic just before emission, i.e. with expected-on wire address w.r.t. to RH* and HAO.

5.1.2.2. Incoming traffic

TOC

When an incoming IPsec packet is handled by IRO, as the last step before being processed by the IPsec module, the SPI is used as the main key to find existing source and destination addresses remapping rules for that traffic (at most one for each).
Each rule has an expected on-wire address. The expected address is checked against the on-wire one found in the packet. If it matches, the remapping occurs. Note that the remapping rules for source and destination addresses are applied in an independent fashion.

5.1.2.3. Outgoing traffic

TOC

When an outgoing IPsec protected packet is handled by IRO, the SPI is used as the main key to find existing source and destination addresses remapping rules for that traffic (at most one for each). The expected address is checked against the one found in the IPv6 header of the packet. If it matches, the remapping occurs. Note that the remapping rules for source and destination addresses are applied in an independent fashion.

5.1.2.4. Related traffic (ICMPv6 error traffic, fragments)

TOC

5.1.3. MH traffic

TOC

MH traffic emitted and received by a MIPv6 entity using IRO has specific additional requirements compared to common data traffic exchanged between those MIPv6 entities.
Basically, the checks and settings on source and destination addresses are relaxed to allow IPsec-protected traffic sent from a new non-registered CoA to pass through. In the MIPv6 stack of the CN, checks are done using an ancillary path that allows the on-wire address to be passed for verification.
Here, we only consider IPsec-protected traffic associated with transport mode SAs whose selectors provide protection of MH traffic. Granularity considerations are covered below.
The search for remapping rules is done in the same fashion as previously described for data traffic. Only checks and application of the rules are changed as described below.

5.1.3.1. Incoming traffic

TOC

If a remapping rule is found for source address, which contains the unspecified address as check, the remapping is performed without checking the source address of the packet. The unspecified address is used as a wildcard.
In source rule case, the on-wire address found in the packet is stored as an ancillary data for further processing and decision by the MIPv6 stack (commonly in userland).
Note that this specification does not explicitly mandate when the unspecified address should be used in the source remapping rule, and leave that to implementors, as it is highly dependent of following facts:

- if the system does not support fine-grained SP/SA or simply does not use them for MH traffic with a peer, then the use of the unspecified address will be required.
- if fine-grained SA are used, the MIPv6 stack will use the unspecified address if the traffic received protected by that SA can't be reliably mapped to a specific CoA for the peer, i.e. if it is expected and authorized that the peer sends traffic from another [possibly to be registered] CoA. This is the case for BU, AOTO, AOTR traffic for instance.
- if the MIPv6 stack supports extensions to [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.)-defined MH messages, the use of IRO will still remain possible with those extensions.

Note that this decision is not expected to create interoperability issues, as the use of the unspecified address is based on non-ambiguous criteria defined in the documents specifying the purpose of MH traffic. Also note that the use of the unspecified address for checks and the passing of the on-wire address to the MIPv6 stack for further processing is equivalent from a security standpoint to the decision that occurs in common MIPv6 processing of HAO extension.

5.2. Rules syntax

TOC

To avoid long descriptive sentences in following section, a simple syntax for expressing remapping rules is provided here.

5.2.1. Remapping rules content

TOC

A remapping rule is made of:

- a direction, describing the kind of traffic it will potentially be applied to. Possible values are "incoming" or "outgoing"
- an SPI value, distinguishing the IPsec packets, encountered in that direction, to which the rules might apply.
- a value for expected source address or destination address, that will be respectively compared with the content of the source or destination address field in the IPv6 header.
- For a source address, the unspecified address (::) is used as a wildcard, in which cases all addresses are allowed.
- a value for source or destination address, that will be used for remapping the associated address in the packet. If a single address is provided, it is used for remapping after checks have been performed.

  If the special keyword "ancillary" is used for remapping a source address, the address to be used is found as an ancillary data in the packet.

  If the keyword "(ancillary)" appears next to the address to be used for remapping a destination, the remapped address should be copied as ancillary data in the packet (see example 4 in next subsection).

5.2.2. Remapping rules simple syntax

TOC

This subsection defines a simple syntax for providing the content described in previous subsection. Those are given as a set of examples with few comments.

1. A typical set of remapping rules found on a MN (HoA, CoA) for a protected data flow with a CN available at address A:

dir: out, SPI: 42, exp. src: HoA, remap. src: CoA
dir: in , SPI: 43, exp. dst: CoA, remap. dst: HoA

2. A typical set of remapping rules found on a MN (HoA, CoA) for protected MH flows with a CN available at address A:

dir: out, SPI: 44, exp. src: HoA, remap. src: CoA
dir: in , SPI: 45, exp. dst: CoA, remap. dst: HoA

3. A typical set of remapping rules found on a MN (HoA1, CoA1) for a protected data flow with another MN (HoA2, CoA2):

dir: out, SPI: 46, exp. src: HoA1, remap. src: CoA1
dir: in , SPI: 47, exp. dst: CoA1, remap. dst: HoA1
dir: out, SPI: 46, exp. dst: HoA2, remap. dst: CoA2
dir: in , SPI: 47, exp. src: CoA2, remap. src: HoA2

4. A typical set of remapping rules found on a MN (HoA1, CoA1) for protected MH flows with another MN (HoA2, CoA2):

dir: out, SPI: 48, exp. src: HoA1, remap. src: ancillary
dir: in , SPI: 49, exp. dst: CoA1, remap. dst: HoA1
dir: out, SPI: 50, exp. dst: HoA2, remap. dst: CoA2
dir: in , SPI: 51, exp. src: ::, remap. src: HoA2 (ancillary)

Note that in example 4, last rule expresses the "blind" remapping of source address to HoA2; the remapped address is passed as ancillary data for further check by the MIPv6 process.

---

6. Tracking SPI changes

TOC

[Following discussions are only geared towards unicast traffic and the whole section will certainly get more accurate/interesting information during implementation of the mechanism]
With IRO, the SPI values referencing SAs are of primary importance: their correct collect and tracking in the time is a requirement to allow remapping rules to be kept in sync with the changes that can occur in the IPsec stack or MIPv6 stack. One important remark is that the actions performed by the IRO part of the MIPv6 stack on incoming and outgoing IPsec protected packets is completely transparent for the IPsec stack. There is no initial requirement for the IPsec stack

associated with the use of IRO (even if having IRO implemented in the IPsec stack might be beneficial).
IRO acts at the lowest possible level, theoretically just outside the IPsec stack, directly on the IPsec protected packets, and only requires access to three pieces of information to track and filter that packets: SPI, source and destination addresses.
This section covers that tracking and associated actions based on the availability of PF_KEYv2 API [RFC2367] (McDonald, D., Metz, C., and B. Phan, “PF_KEY Key Management API, Version 2,” July 1998.). The intent is to base the discussion on a standard interface but it generally apply in a system dependent fashion to other interfaces (Netlink/XFRM, ...). It obviously rely on the synchronisation between the two IPsec stacks on peers (SADB mainly, expected to be done by IKE).

6.1. Initial collect ?

TOC

[The need for initial collect _clearly_ depends on the location of IRO engine is implemented and how remapping rules are pushed/changed]
The way remapping rules are put in place and maintained on the system implementing IRO is a local matter. The only requirement is that the externally understood behavior be in sync with the description provided in the document. This is especially important with changes associated with registration/deregistration and movement.
In that context, if IRO engine is running in userland, there might be a need for maintaining a limited local version of system's SADB to be able to efficiently manage changes (removal, addition, CoA change) against a set of SA. For instance, when an IRO registration is accepted for a peer, remapping rules are put in place to have its HoA remapped to the CoA for incoming IPsec traffic (and the reverse for outgoing IPsec traffic). Upon movement, all those remapping rules must be updated to reflect the change of CoA.
In that case, the use of PF_KEY SADB_DUMP message is possible to get access to the whole SADB content, filter interesting SA, load required remapping rules for those SA (as described for PF_KEY SADB_UPDATE message in 6.2.1) and initially populate some initial IRO SA state table.
Then, if used, this table could be updated when receiving PF_KEY messages described in following subsection (addition or removal of entries), during movement (access to all impacted SA whose remapping rules should be remapped), or during registration/deregistration (addition/removal of associated remapping rules).

TOC

6.2. SADB related PF_KEY events

This subsection covers the actions performed by IRO when receiving SA related PF_KEY events. Those actions deal with the filtering of interesting SAs and installation/removal of associated remapping rules. If another interface than PF_KEY is used to track SA related events (or IRO logic is not implemented in userland), the behavior of IRO must remain the same with regard to the addition/removal of remapping rules.

6.2.1. Overview

TOC

A fundamental need of IRO is associated with the ability to setup remapping rules _before_ traffic that use those rules is emitted. A direct impact of this requirement is the need to access the SPI of the SA that will protect the traffic _before_ that SA is used. In practice, when dynamic keying is used, this creates an interesting challenge: because SA negotiation is usually triggered by a packet matching a SP, and IRO does not modifies IKE processing, some care is required in the implementation to ensure that the SPI information is gathered and the associated remapping rule installed _before_ the triggering packets is IPsec- and then IRO-processed.
When dynamic keying is implemented using PF_KEY framework, the sequence of events performed by the key manager allows to implement that behavior, basically by monitoring SADB_GETSPI messages from the kernel in order to access SPI value and install the remapping rule while the SA is being negotiated.
It is an implementation issue to ensure that IRO will be able to access the SPI and install the remapping rules before they are used. This highly depends on the location of IRO implementation (userland, kernel space), framework (PF_KEY, ...), ...

6.2.2. Reception of a PF_KEY SADB_GETSPI message

TOC

When the kernel returns a PF_KEY SADB_GETSPI message to all listening processes, IRO processing engine considers this kernel message. After validation (kernel emitted, errno not set, ...), it extracts the interesting information from the message (SA, Addresses, SPI) in order to decide if remapping rules are needed for this SPI.

TOC

6.2.3. Reception of a PF_KEY SADB_UPDATE message

When the kernel returns a PF_KEY SADB_UPDATE message to all listeners, following reception of the message from a key manager, IRO processing engine considers this kernel message. After validation (kernel emitted, errno not set, ...), it extracts from it the Source and Destination address extensions along with the direction and the SPI value found in the association header.
Direction allows to decide if the remapping rule is an incoming or outgoing one. proto values (should match) allow to decide if wildcard rules are required (MH case). As there is more granularity available with IKEv2 selectors, this implies more cases and more specific rules (based on MH Type). [This part will get the required level of precision during the implementation]. Addresses allow to decide if an address is our HoA for which a peer has registered our CoA, or the HoA of a peer for which we have registered its CoA.

6.2.4. Reception of a PF_KEY SADB_ADD message

TOC

From IRO standpoint, SADB_ADD message is processed in the same fashion as SADB_UPDATE message. The message returned by the kernel to all listening processes contains the required SPI (in association header) along with the source and destination address extensions.

6.2.5. Reception of a PF_KEY SADB_DELETE message

TOC

The reception of a PF_KEY SADB_DELETE message from the kernel must trigger the removal of associated remapping rules for the SA if any (i.e. having that SPI).

6.2.6. Reception of a PF_KEY SADB_EXPIRE message

TOC

When IRO engine receives a PF_KEY SADB_EXPIRE message from the kernel for a SA for which it has loaded some remapping rules, the associated action depends on the kind of expiration (hard or soft limit):

- In soft case, nothing is done as the SA is still valid.
- In hard case, the SA may already have been deleted from the SADB and IRO engine must remove associated remapping rules.

6.3. Rekeying

TOC

6.3.1. Phase 2

TOC

When dynamic keying is used, negotiated IPsec SA have limited lifetime. With IKEv1, the lifetime is negotiated and the rekeying is performed by the initiator. In the context of MIPv6, this is expected to be the peer.
As stated in Section 2.8 of [RFC4306] (Kaufman, C., “Internet Key Exchange (IKEv2) Protocol,” December 2005.), a "difference between IKEv1 and IKEv2 is that in IKEv1 SA lifetimes were negotiated. In IKEv2, each end of the SA is responsible for enforcing its own lifetime policy on the SA and rekeying the SA when necessary. If the two ends have different lifetime policies, the end with the shorter lifetime will end up always being the one to request the rekeying". Again, in the context of MIPv6, it is expected that the MN will be the initiator that will perform the rekeying (i.e. having the shortest lifetime).
In both cases, independently of the specific details of rekeying process, new SA will be put in place with new SPI values. When this event occurs on one side, IRO implementation will get _live_ information regarding the installation of new SAs by receiving PF_KEY SADB_ADD messages. It will be followed after some time by the reception of PF_KEY SADB_EXPIRE messages indicating the expiration of a "hard lifetime" for old SAs.
From IRO's perspective, IPsec SA rekeying process is only seen through the reception of specific PF_KEY messages for which associated actions have previously been described.

7. Extending advantages of IRO to the HA

TOC

7.1. Rationale and expected advantages

TOC

IRO's primary purpose is to improve security and efficiency of MIPv6 communications in IPsec environments. Because most of them are expected to occur directly between peers, IRO is oriented towards MN-CN and MN-MN flows.

But the flows between a MN and its HA can also benefit from the improvements: using the SPI information available on both sides to perform the remapping of incoming and outgoing IPsec traffic, the need of RH2 and HAO extensions between the MN and its HA simply disappears. This provides anonymity (See Appendix J (Anonymity)) of the MN on a foreign link by hiding its HoA to eavesdropper on the path (if IKE does not leak that information). It also makes the MN fully capable in networks were only IPsec is allowed to flow (500/udp is required for the initial negotiation of SA and infrequently for rekeying).

7.2. Changes to HA processing

TOC

IRO does not mandates a detection mechanism (Appendix I (Rationale for not specifying a new BU)) and transparently reuses most of [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.)-defined messages. For that reason, MN and HA must be explicitly configured to use IRO.
The changes to HA processing for the peer, required by the use of IRO, are simply the use of remapping rules instead of HAO and RH2 extensions.
With IRO, the relationship between a MN and one of its CN is basically the same as the relationship between the MN and its HA, with the following simple differences:

- HA and MN never exchange AOT* messages as the MN is always trusted regarding the CoA information it provides in its BU.
- HA and MN have a larger set of possible messages they can exchange. Remapping rules should be able to handle that.
- Chances are high that an IPsec tunnel be used for protecting traffic relayed through the HA. Remapping rules do not interfere with that as the associated SA is not tracked. This is due to the fact that the SA references the CoA of the MN as the source (on-wire) address of the communication and not the HoA.

7.3. Changes to MN processing

TOC

The changes to MN processing for IRO to be used with its HA are quite comparable to the one previously described for the MN, i.e. they are naturally deduced from the basic requirement that RH2 and HAO must be replaced by the use of remapping rules.

8. Implementation Notes

TOC

The content of this section is not meant to be normative but only informative.
This section provides some explicit feedback associated with the implementation of IRO on Linux (Linux kernel, UMIP mobility daemon and racoon IKE daemon). Based on the specific targeted system, some of the points discussed in this section may be completely irrelevant.

8.1. Nested SA

TOC

8.1.1. Problem

TOC

The main purpose of IRO is to route optimize IPsec traffic exchanged between the MN (from its HoA) and its CN. Before that optimization takes places (i.e. before the AOT* exchanges), that traffic is expected to follow the natural path, i.e. be routed via the tunnel to the HA. In IPsec environments, chances are high the data path to the HA will be IPsec protected, using IPsec in tunnel mode as (optionally) expected by MIPv6 specifications. In that case, before the optimization is effective, traffic sent by the MN to the remote IPsec peer will have to undergo both the protection of the specific SA protecting the end-to-end traffic with the peer and the tunnel one protecting the data traffic to the HA. This is required (at least for topological reasons) because the HoA is only valid as an inner address for tunneled traffic. This is basically the kind of setup described in Appendix E of [RFC4301] (Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” December 2005.).
Supporting that kind of nested IPsec configuration, even temporarily before the route optimization is in place, is not straightforward. Obviously, this usually does not require anything specific on the HA or the CN, but the MN case may be trickier.
In the specific context of IRO, there may be a need for both previously described IPsec SP/SA to exist separately. The main reason is that, even if the traffic to the CN initially needs to undergo both SP (and in the end protection provided by associated SAs), this need disappears when the optimization is in place. At that moment, the traffic only undergo the end-to-end SP and the protection of associated SA.

8.1.2. Selected solution

TOC

XXX FIXME

8.2. Having IKE traffic flow via the IPsec tunnel to the HA

TOC

8.2.1. Problem

TOC

Traffic generated by an IKE daemon needs to bypass the system's security policies in order to avoid chicken and eggs issues. Unix IKE daemons implementation usually achieve that using a specific IPsec bypass setsockopt() call on their sockets.
In common situations, previous method works just fine. But when an IPsec data tunnel already exist on the system as it is usually the case for corporate VPN clients, this method prevents the use of the inner tunnel address for IKE negotiation with remote peers accessible only via the remote security gateway (e.g. hosts in the corporate network). Stated differently, this prevents the setup of end-to-end IPsec protection via the IPsec tunnel.
More precisely, if the IKE daemon tries and use the inner address for negotiation with a peer, the IPsec bypass setsockopt() call on associated socket prevents associated IKE traffic to flow correctly. This is because, from a topological standpoint, the only valid path for traffic originating from that address is via the IPsec tunnel.
When MIPv6 data traffic between the MN and its HA is required by policy to undergo IPsec tunnel protection, the same limitation as described above exists. For the specific needs of IRO, this is an issue because the HoA is used for the IKE negotiation with the CN (whose side effect is also to prove HoA ownership to the peer).

8.2.2. Selected solution

TOC

For the sake of the discussion, we consider the existence of some wide IPsec SP requiring protection of all traffic from the HoA to a given peer behind the HA. To make things clear, IKE traffic (500/udp) between the HoA and the address of the peer matches this SP's selectors.
Obviously, the simple removal of the IPsec bypass setsockopt() on the socket associated with the HoA is not sufficient to make things work. This would have initially been sufficient to have associated IKE

traffic undergo the IPsec tunnel mode SP (protecting data traffic between the MN and its HA). But the existence of the additional SP creates a chicken and eggs situation and prevents things to work that easily.
But once the IPsec bypass setsockopt() call is removed for the IKE socket associated with the HoA, associated traffic basically undergo the system security policies. Then, the addition of a high priority SP with selectors specifically suited for IKE traffic from the HoA to the address of the peer is sufficient to have the IKE traffic be IPsec tunneled using the existing SA already protecting MIPv6 data traffic.
From an implementation perspective, the removal of the IPsec bypass setsockopt() call has been implemented by adding a simple option ('no_bypass') to the racoon IKE daemon allowing the user to specify an address for which associated socket should not undergo the setsockopt() call.
With regard to the addition of the high priority IPsec security policy matching IKE traffic between the HoA and the address of the peer, it was easier to have that job done inside UMIP. This is basically because UMIP is already the one handling the installation of other security policies for MIPv6 and data traffic. Another reason is that UMIP will need to update the tunnel mode SP after a handover. (via [MIGRATE] (Ebalard, A. and S. Decugis, “PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE,” August 2008.)).

8.3. Remapping rules and old IPsec architecture

TOC

8.3.1. Problem

TOC

XXX FIXME: the old IPsec architecture expected SAD lookups to be performed by SPI and destination address. If an IPsec stack only implements such kind of lookups when handling IPsec traffic, this may require additional work to support the implementation of IRO remapping rules. [RFC4301] (Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” December 2005.) changed that behavior and now expects SAD lookups for unicast SA to be performed by SPI, which is expected to simplify the implementation of IRO remapping process.

8.3.2. Selected solution

TOC

XXX FIXME

9. Security Considerations

TOC

9.1. Proof of address ownership

TOC

9.1.1. Position of the problem

TOC

As a CN, registering a binding between a CoA and a HoA is not something harmless. This can be seen as a modification of local routing table, like an order from a peer to direct traffic to a specific address. For that reason, the CN needs some proof regarding this binding. In MIPv6, RRP has been designed with the hypothesis that there is no initial trust relationship between a MN and its CN. The solution to provide confidence to the CN in the HoA and CoA binding has consisted in showing the ability for the MN to send _and_ receive traffic both at the HoA and CoA.
With IRO, there is an initial trust relationship between a MN and the CN it will contact. This is expected to take the form of cryptographic credentials (X.509 certificates, ...) that will allow an IKE negotiation to occur to setup SAs to protect the binding. Static keying case is covered in Appendix G (Compatibility with static keying). Those SA only references the HoA of the MN and not at all its CoA.
The point here is that the existence of SAs does not directly provide to the CN any _live_ proof of address ownership as it occurs with RRP. Furthermore, as summarized in section 6.2 of [RFC4866] (Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” May 2007.) paragraph 4, the trust relationship between a HA and its MN is very different from the one between a MN and a CN, even if both use IPsec/IKE to authenticate.

9.1.2. Home Address ownership

TOC

The proof of HoA ownership to the CN is one of the reason behind the design decision to have MN and CN perform the IKE negotiation via the tunnel to the HA (i.e. using the HoA). That way, the existence of the SAs gets bound to a successful initial exchange between the CN and the

MN. This proves to the CN the ability for the MN to send/receive traffic from/at that address.
Nonetheless, as IKE basically allows negotiation to be performed from a different address than the one the SA contain ([MIGRATE] has such an use), this behavior MUST be prevented on the CN for the purpose of negotiations of the initial SAs that will protect MH traffic for IRO's binding between the MN and the CN.
While MN and CN are able to perform an IKE exchange between them using a set of credentials, there are many possible reasons for which those credentials might in fact be invalid at the time the negotiation occur. This might for instance be the case if the CN has not up to date revocation information. This can also result from the use by the MN of a different set of credentials for the purpose of protecting its HA registration and the registration with its CN.
Mandating the IKE negotiation to be routed through the tunnel to the HA provides the proof that the MN is still granted ownership of the address by the network it belongs to at the time of negotiation. It should be noted that the proof of HoA ownership occurs at SA setup time and remains valid till the SA is rekeyed, i.e. each rekeying providing a new live proof. This specification does not mandates regular check of HoA ownership between rekeying. Appendix C (Arguments for no regular check of HoA ownership) provides arguments on that topic.
The case of static keying is covered in Appendix G (Compatibility with static keying).

9.1.3. Care-of Address ownership

TOC

The proof of CoA ownership by the CN is an especially important point in the security of large scale deployments of IRO. As stated in the introduction of this section, the acceptance of a binding by a CN for a CoA is a local modification of local routing table to send current and future traffic to that address when it is destined to the HoA.
The proof by the MN that it is able to both send and receive traffic at this address is a primary concern in the security of the protocol. Appendix A (Ability to send does not prove CoA ownership) covers the reasons why the only ability to send is an insufficient proof of CoA ownership, even in the context of IRO.

9.2. Remapping (comparison with explicit HAO/RH2 inclusion)

TOC

For every remapping, the practical impact is the same as the explicit one resulting from the inclusion of a RH2 or HAO.

9.3. Anonymity

TOC

At the moment, this section is empty. See Appendix J (Anonymity).

9.4. Limiting attack surface

TOC

IRO can provide the ability to have port 500/udp open for remote negotiations on the HoA for the purpose of the inbound contacts and not on the CoA. CoA is only used for the discussion between the MN and its HoA, which allow to put some specific firewalling rules in place for that purpose.

---

10. IANA Considerations

TOC

The values for following mobility header messages MUST be assigned by IANA:

- *Address Ownership Test Offer message (AOTO, see Section 4.4.1 (Address Ownership Test Offer (AOTO)))
- *Address Ownership Test Challenge message (AOTC, see Section 4.4.2 (Address Ownership Test Challenge (AOTC)))
- *Address Ownership Test Response message (AOTR, see Section 4.4.3 (Address Ownership Test Response (AOTR)))
- *Address Ownership Test Status message (AOTS, see Section 4.4.4 (Address Ownership Test Status (AOTS)))

The values for following mobility option MUST be assigned by IANA:

- *Nonce Option (see Section 4.3.1 (Nonce option))

---

11. Acknowledgements

TOC

The author acknowledge the comments and correction of Guillaume Valadon on the initial version of the document.
This document was generated by xml2rfc.

12. References

TOC

12.1. Normative References

TOC

[RFC2119]	Bradner, S., “"Key Words for Use in RFCs to Indicate Requirement Levels",” RFC 2119, March 1997 (TXT).
[RFC2367]	McDonald, D., Metz, C., and B. Phan, “PF_KEY Key Management API, Version 2,” RFC 2367, July 1998 (TXT).
[RFC2409]	Harkins, D. and D. Carrel, “The Internet Key Exchange (IKE),” RFC 2409, November 1998 (TXT).
[RFC3775]	Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” RFC 3775, June 2004 (TXT).
[RFC3776]	Arkko, J., Devarapalli, V., and F. Dupont, “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents,” RFC 3776, June 2004 (TXT).
[RFC4301]	Kent, S. and K. Seo, “Security Architecture for the Internet Protocol,” RFC 4301, December 2005 (TXT).
[RFC4303]	Kent, S., “IP Encapsulating Security Payload (ESP),” RFC 4303, December 2005 (TXT).
[RFC4306]	Kaufman, C., “Internet Key Exchange (IKEv2) Protocol,” RFC 4306, December 2005 (TXT).
[RFC4835]	Manral, V., “Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH),” RFC 4835, April 2007 (TXT).
[RFC4877]	Devarapalli, V., “Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture,” RFC 4877, April 2007 (TXT).

12.2. Informative References

TOC

[CNIPsec]	Dupont, F. and JM. Combes, “Using IPsec between Mobile and Correspondent IPv6 Nodes,” draft-ietf-mip6-cn-ipsec-08 (work in progress), August 2008 (TXT).
[MIGRATE]	Ebalard, A. and S. Decugis, “PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE,” draft-ebalard-mext-pfkey-enhanced-migrate-00 (work in progress), August 2008 (TXT).
[RFC4225]	Nikander, P., Arkko, J., Aura, T., Montenegro, G., and E. Nordmark, “Mobile IP Version 6 Route Optimization Security Design Background,” RFC 4225, December 2005 (TXT).
[RFC4651]	Vogt, C. and J. Arkko, “A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization,” RFC 4651, February 2007 (TXT).
[RFC4866]	Arkko, J., Vogt, C., and W. Haddad, “Enhanced Route Optimization for Mobile IPv6,” RFC 4866, May 2007 (TXT).
[RFC4882]	Koodli, R., “IP Address Location Privacy and Mobile IPv6: Problem Statement,” RFC 4882, May 2007 (TXT).

Appendix A. Ability to send does not prove CoA ownership

TOC

With IRO, negotiation of the protection for the registration traffic between the peers is done using the tunnel to the Home Agent (i.e. the HoA). Then, the protected Binding Update message is emitted by the MN. It locally uses the HoA but a remapping process makes the CoA the address appearing on the wire for this packet. When the CN receives that packet, the address is remapped to the HoA of the MN by the MIPv6 stack. The remapped address appearing as source of the packet is passed as ancillary data to the MIPv6 process where a check will be performed during parsing against the content of the required Alternate Care-of Address option.

This process proves the CN that the MN is able to _send_ traffic using the CoA.

Then, IRO requires additional steps for the MN to prove its ability to receive traffic at that address. This appendix covers the threats prevented by the addition of this proof of reception capability in IRO. The trust model between the MN and its HA is based on the existence of the IPsec protection between the two. The only requirement for the update of the tunnel endpoint when a movement occur is the reception by the HA of a protected Binding Update message containing the new CoA in the Alternate CoA option. The use of the new CoA as source of the packet is not even mandatory.

One would argue that the same kind of trust relationship exists between the MN and its CN as they already have an established trust relationship, materialized by the pair of SA protecting MH traffic. Nonetheless there are many difference between the two situations.
The first and main one is that all the traffic emitted by the HA to the CoA provided by the MN has a traceable source: the address of the HA, which belongs to the home network. It allows to track the source of the traffic emitted to the CoA back to the Home Network. In the context of the flow from the CN to the MN, the source address might possibly be that of a foreign network (if the CN is also acting as a MN) and the destination is the one that would be provided by the MN.
Now consider the following, still in the context of a proof of address ownership based solely on the ability of the MN to emit traffic from the CoA. A MN has been compromised by an attacker that has the ability to emit traffic with the address of a target (no ingress-filtering by its provider). The attacker would now be able to mount connections with the HA and then, using IRO, with all the peers that trust the MN. At the moment, it still uses some valid address where it can emit/receive traffic from/to. After having some traffic intensive connection running with a peer, it simply warns the peer of a change of CoA by advertising the address of the target. As the CN does not require a proof of reception capability, all the IPsec traffic gets redirected to the target. This might not be a problem with a single peer and some connected protocol but it is expected that the protocol be used in vast trust domains where the number of peer is not directly limited.
In the end, requiring that the proof of CoA ownership includes a proof of reception capability by the MN at the CoA prevents that compromise of a MN by an attacker provides her with a potentially unlimited number of anonymous and unwilling "bots" to DoS a target other than herself.
In the design of IRO, to maintain the efficiency of the protocol in term of latency associated with movement, the proof of reception capability is not required to occur before the CN can emit traffic to the CoA.

Appendix B. IKE exchanges use the HoA and the tunnel to the HA

TOC

Remainder: in this appendix, we still consider that the data tunnel between the HA and the MN is IPsec protected. Some security arguments in this appendix should be modulated if this hypothesis is known to be invalid.
We provide here some arguments regarding the use of the HoA for performing the IKE exchanges with the peers, using the tunnel through the HA.
The first simple rule which always applies with IRO is that no connection happens directly if it is not IPsec-protected. No difference

is made for IKE exchanges even if those flows have intrinsic protection mechanisms.
The need for performing IRO to get direct routing between the peers is motivated by the net performance impact in terms of bandwidth, delay and jitter by avoiding triangular routing and the bottleneck of HA. This is of interest for specific flows like VoIP, direct file exchanges, ... but are mainly useless for infrequent flows like IKE negotiations. When a MN performs IKE negotiation with a peer, having IKE_SA (or ISAKMP SA for IKEv1) set up is only a matter of few packets (IKEv1 Main mode exchange uses six). Then, all next CHILD_SA (or IPsec SA for IKEv1) will reuse the same IKE_SA and generally complete after a three packet exchange. As rekeying is supposed to occur extremely infrequently and does not need the advantage of direct routing, this is unneeded. The argument regarding the loss associated by the routing through the tunnel gets the same answer: the impact is very limited given the amount of traffic. Furthermore, when certificates are used, IKE packets already get fragmented even with a full 1500 bytes PMTU.
In fact, the advantage of using the HoA and the IPsec tunnel to the HA for performing IKE negotiation with peers is the stability guaranteed by the migration process when movement occurs. MIPv6 simply makes things transparent for all IKE daemon connections from the HoA.
To conclude and after all previous functional arguments, there are also some security advantages in performing IKE negotiations with peers using the protected IPsec tunnel to the HA.
The most important one is anonymity. A positive side effect of having the negotiation performed through the IPsec tunnel to the HA (ESP with meaningful encryption is assumed) is that it hides everything to people in MN's network. IKE traffic is only accessible on the path between the HA and the peer. In fact, in the MN-MN situation eavesdroppers on both foreign networks are unable to get the HoA of the peer on the other network. It requires being on the path between the two HA. The same is also true for the identity information that might appear during the IKE negotiation depending on the modes peers use.
Another security advantage with that policy is that a peer is able to statefully filter 500/udp traffic received on its CoA and allow only outbound initiated connections addressed to the HoA. This policy simply allows reducing the network attack surface of the node in the foreign network.

Appendix C. Arguments for no regular check of HoA ownership

TOC

As presented in Section 9.1.2 (Home Address ownership), when dynamic keying is used, the initial IKE negotiation protecting the registration traffic between the MN and the CN provides to the CN the proof of HoA ownership by the MN. This proof remains valid till this SA is rekeyed. This is also true for further SA negotiated between the MN and the CN.

The initial proof of HoA ownership is easily obtained as it results from a positive information: packets exchanged with the MN at this address. Note that the inability for the MN or the CN to get traffic routed to the HA at that moment results in the inability to get direct connectivity as the IKE negotiation cannot be performed. In the same fashion, after the initial proof, there is no defined way to track a loss of HoA ownership through a positive event: the CN is simply not warned that the MN has been removed ownership of its HoA by its home network (resulting from a compromise, change of network prefix, ...). Discovery of a loss of HoA ownership cannot be tracked by a negative event either, such as the inability to exchange traffic with the MN at a specific moment. In fact, a crash of the HA, the loss of connectivity between the MN and its HA, or between the CN and the HA are to be expected. In that context, such a mechanism would simply amplify the existence of points of failure or allow DoS to occur. Avoiding that provides resilience and allow direct communications to survive previous failure conditions related to the HA.
Another reason to prevent regular proof of HoA ownership is the use of the HoA in IRO. It acts as a local identifier on both peers. It allows the MN to acquire movement independence and can be seen as a convenience in the relationship between the peers, to find themselves initially, no matter where they are located. With IRO, the HoA never appears anymore in packet exchanged directly between the peers (due to removal of HAO and RH2). It is only understood locally in the context of ongoing IPsec communications between the peers.
The last argument for not including this requirement (capability is provided, see Section 4.5.3 (Test of HoA ownership)) in the protocol is that different CN or MN might have different more efficient methods for performing that tracking. For instance, inside a home network, instead of using a constant regular polling by all MNs, an administrator revoking the credentials of a MN will easily be able to request all MNs to update their revocation information, before shutting down communications with associated MN (i.e. replacing polling by push).
In the context of IRO, no mechanism to perform regular checks of HoA ownership is included. This capability is outside the scope of this specification.

Appendix D. Lack of encryption between MN and HA

TOC

In this specification, the use of IPsec tunnel protection of data traffic is expected. Note that section 5.5 of [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.) only specifies that:

> For traffic tunneled via the home agent, additional IPsec ESP encapsulation MAY be supported and used. If multicast group membership control protocols or stateful address autoconfiguration protocols are supported, payload data protection MUST be supported.

The logic behind previous expectation is associated with the availability of credentials between the MN and HA, and also the kind of environment in which it will get deployed.
However, the lack of IPsec protection of tunneled data does not prevent IRO; it only removes some security advantages of this protection. This loss is covered in this appendix.
When negotiating IRO, the MN uses the tunnel to its HA for routing IKE negotiation with the peer. As IKE is designed for robustness, the advantage of the privacy when IPsec is used for protecting the data tunnel (i.e. non NULL encryption) is the insurance that the address of the peer or its cryptographic credentials are not disclosed on MN's network. Note that MN's HoA and associated identity are expected to be disclosed to eavesdroppers during registration of the MN to its HA (if IRO is not extended to HA-MN exchanges).
As a conclusion, removing the hypothesis of privacy for data tunneled to the HA removes the anonymity provided to peer's identity (HoA or CoA, and possibly cryptographic identity appearing during IKE exchange).

Appendix E. What if I don't need protection?

TOC

IRO mandates the use of IPsec for all direct communications between MIPv6 peers. As IPsec is only a framework, the level of protection might vary, along with the additional requirements, environments and capabilities of end devices.
There will certainly be some very specific and limited cases where people will see a need in downgrading the security for performance or other reasons. To be fair, except in some very specific conditions, achieving performance while still keeping security is possible. For instance, if authentication is a real requirement but privacy is not (but it is still activated by default), and CPU limits the throughput, keeping only authentication services of IPsec as provided by ESP with NULL encryption or by AH will clearly boost performance.
Now, if there is a desperate need to suppress security services between MIPv6 peers for some reason, the best thing is to use another route optimization like common RO as specified in [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.), instead of trying to circumvent them.

For those with some imagination, who still think the author is wrong and think about simply negotiating NULL authentication and NULL encryption, next paragraph might be worth reading. [RFC4835] (Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)," April 2007.) defines mandatory-to-implement cryptographic algorithms for use with ESP (and AH). NULL encryption algorithm and NULL authentication algorithm must both be implemented. In section 3.2 of [RFC4303] (Kent, S., "IP Encapsulating Security Payload (ESP)," December 2005.), some requirements are specified on those algorithms, preventing their simultaneous uses:

> Note that although both confidentiality and integrity are optional, at least one of these services MUST be selected, hence both algorithms MUST NOT be simultaneously NULL.

Appendix F. MTU Gains

TOC

Standard RO is based on the use of RH2 and HAO to explicitly carry the HoA of the MN, respectively as real destination or final source of the packet sent directly between the nodes:

- *From MN to CN: HAO
- *From CN to MN: RH2
- *From MN to MN: HAO and RH2, simultaneously.

The inclusion of these explicit containers generates a loss of MTU. In common case, where no other specific extensions or options are used (to remove padding considerations), HAO and RH2 each consume 24 bytes. The loss of MTU associated with those MIPv6 extension for direct MN-CN communications is 24 bytes. For direct MN-MN communications, it is 48 bytes. As an initial comparison, unprotected routing via the HA through an IPv6-in-IPv6 tunnel consumes 40 bytes. When an IPsec tunnel is used, the loss of MTU depends on the authentication and encryption algorithm, negotiation of ESN, padding requirement.
As IRO has been designed to provide secure IPsec-protected direct communications between MIPv6 peers, it is difficult (and does not make that much sense) to compare the loss of MTU associated with IRO and the one of standard unprotected RO. In term of header inclusion, IRO neither use RH2 nor HAO but require AH or ESP. Depending on the size of ESP or AH header(s) and the specific type of communication (MN-MN or MN-CN), one route optimization type might consume more bandwidth than

the other:

- *ESP in transport mode using HMAC-SHA1-96 (required in all implementation) as authentication algorithm, NULL for encryption and no ESN consumes 24 bytes (with 2 bytes of padding). Adding a meaningful encryption algorithm will make that higher.

- *AH in transport mode also using HMAC-SHA1-96 and no ESN will give a similar value.

To make things simple, using IRO with some ESP with NULL encryption or with AH for MN-CN communications provides similar MTU loss as standard RO. Having a meaningful encryption algorithm (expected) with ESP give a little advantage to standard RO regarding MTU loss.
When considering MN-MN, IRO will clearly consumes less bandwidth than standard RO in all possible combinations of algorithms for AH or ESP. Now, considering the same level of protection, i.e. by using IPsec for standard RO carried packets (we do not take into account padding variations), IRO simply gets a direct advantage: 24 bytes for MN-CN communications and 48 bytes for MN-MN communications. It is due to the complete removal of HAO and RH2 from packets exchanged directly between peers.
In fact, regarding MTU considerations, IRO provides a zero cost mobility service to IPsec protected connections between end nodes.

Appendix G. Compatibility with static keying

TOC

IRO has been designed for enabling direct secure communications between MIPv6 entities belonging to a common trust domain. Scalability was a primary concern; This is the reason why the specification covers SA negotiation under the hypothesis that IKE is used for that purpose. But IRO is also fully compatible with static keying.
In fact, the specification is not specifically bound to the use of either static or dynamic keying for SA setup; it is left as a local configuration decision to domain administrators.
This appendix quickly covers the differences regarding the use of static keying with IRO.
One great difference between static and dynamic keying is the removal of the IKE negotiation. For IRO, the first negotiation performed with the peer provides an additional information to the CN: a live proof of address (HoA) ownership by the MN. The removal of this step also removes the live check. This is a fact administrators should be aware of.
The question of rekeying is of primary interest for the maintenance of SPI information on MN and CN that use IRO. This changes somehow with static keying as the rekeying is done ... by the user. Even if it is

expected to happen less often, tracking of SA removal and addition, along with their associated SPI is still required. It is expected that the same mechanism (PF_KEY is one of them) used for tracking addition and deletion of SA by IKE be used for that purpose.
There should be no specific reason preventing the simultaneous use of static and dynamic keying with IRO.

Appendix H. Compatibility with the use of CoA in SP/SA

TOC

SP and SA are not changed at any moment by MIPv6 stack when IRO is used. Only incoming and outgoing IPsec packets can undergo source or destination address modifications, mainly based on SPI information.
When using IRO, MIPv6 stack tracks SA addition and deletion looking for local HoA or IRO peers' HoAs (MN) as source or destination addresses of those SA (endpoints for tunnel mode SA). Associated SPI are used for tracking IPsec packets.
Outgoing IPsec packets are only possibly modified to change the HoA into the CoA. CoA of outgoing IPsec packets are never modified by MIPv6 stack, when IRO is used.
Incoming IPsec packets will have their source modified (from CoA to peer's MN HoA) iif the SPI is the one of a tracked SA that expect the HoA of an IRO peer. This implies that no incoming packet with a CoA source will be modified if the SA associated with its SPI references that CoA (and not peer's HoA). Regarding destination address of an incoming IPsec packet, remapping of a CoA will occur if the SA associated with the SPI expects an HoA. This implies that no incoming packet with a CoA destination will be modified if the rules associated with its SPI references that CoA (and not our HoA).
As a conclusion, the work of IRO is compatible with the use of CoA as destination or source address (endpoint addresses for tunnel mode) of any SP/SA.

Appendix I. Rationale for not specifying a new BU

TOC

IRO is not designed as a fallback mode for IPsec communications between MIPv6 entities but as an improved alternative.
You cannot use IRO and common mode with the same peer. You either need the security advantages of IRO for communications with a peer or you can afford unprotected direct communications with it, for which common RO has been developed. Parallel uses of common mode and IRO mode with different MIPv6 entities (including its HA) is not forbidden but strongly discouraged as it suppresses the anonymity of the MN on its foreign link.

For that reasons, IRO does not come with some detection algorithm against peers that do not have IRO activated to perform a fallback to common mode. Considering the setup associated with the protection mechanisms required by IRO and the kind of environments it is expected to be used in, requiring that entities be configured to specifically use IRO for a peer (or by default, preventing the common mode) is required.
This has many positive impacts both on development costs, deployment and debugging. This notably provides the ability to reuse messages without creating parallels versions where needed. As only a few things changes when IRO is activated between two entities, most of the code remains usable. In fact, the two mains changes introduced by IRO are:

*the removal of HAO/RH2 and the replacement by the remapping process on selected IPsec traffic.

a simplified registration procedure with CN (AOT framework)

Let's go a little further. One can think that it would have been possible to create specific mobility options to discriminate IRO mode from the common mode. This was impossible for multiple reason. First, from a specification perspective, section 6.1.7 of [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.) requires that "The receiver MUST ignore and skip any options which it does not understand", which prevents the reuse of MIPv6 messages with a slightly modified semantic if peers are not aware of that. For options to have an interest, you have to be aware that the peer support it (not necessarily that it is activated).
Anyway, there is a better reason that makes the use of common mode and IRO mode incompatible between peers: IRO remapping process must be activated on the receiver for the packets to be valid. If a MN that uses IRO sends an IPsec protected Binding Update message to a peer that is not using IRO, no remapping will occur and the checksum will end up being invalid (if it passes the IPsec stack). Section 9.2 of [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.) requires the following rule to be applied to such packet: "The checksum must be verified as per Section 6.1. Otherwise, the node MUST silently discard the message".

Appendix J. Anonymity

TOC

There are mainly 2 kinds of identifiers that can appear during an IPsec protected communication in IKE/MIPv6 environments: addresses (HoA, CoA, CN addresses) and cryptographic identifiers (IKE credentials, i.e. X.509 certificates).

In MN-CN communications, the addresses of the CN and the CoA of the MN will obviously be disclosed, but they should not be meaningful. We see later that in MN-MN case, the address of the CN that appears on the wire might temporarily be the HoA, before registration has been performed by the second MN.
In MIPv6, the use of explicit containers (HAO and RH2) makes the Home Address of the MN available in all cases. With IRO, the complete removal of this extensions prevents the disclosure of the HoA during direct MN-CN communications and MN-HA communications.
The removal applies to:

* the IPsec protected signaling traffic exchanged directly between the two peers (BU/BA for instance)

* the IPsec protected data traffic exchanged in MN-MN and MN-CN cases (when tunnel mode is not already used to avoid RH2/HAO).

From the perspective of an eavesdropper on the FL of the MN, when IRO is used the visible exchanges that occur are (in order, for MN-MN case, with registrations performed on that link, i.e. worst case scenario):

* IKE negotiation between the CoA of the MN and its HA

* IPsec protected BU/BA exchanges using CoA and HA@ as on-wire addresses (remapping rules applied on both ends)

* IPsec protected (tunnel mode this time) traffic with peers

* IKE exchange from the HoA, IPsec tunneled to the HA, with a CN

* Direct IPsec-protected BU/BA exchanges using the CoA and the address of the the CN for on-wire addresses.

* Direct IPsec-protected data traffic exchange with the CN, between the CoA and the address of the CN.

In all those exchanges, the only addresses that are disclosed to an eavesdropper on the FL of the MN (if ESP with a meaningful encryption is used for all IPsec exchanges) are the CoA, the address of MN's HA and the address of the CN. The HoA of the MN never appears in those exchanges.
For IKE case, even if it is used as an ID in Phase 2 for bootstrapping as described in [MIGRATE] (Ebalard, A. and S. Decugis, “PF_KEY Extension as an Interface between Mobile IPv6 and IPsec/IKE,” August 2008.), the exchanges are encrypted and the HoA does not appear. For the negotiation with the CN, because the HoA is used for the exchanges, the IPsec tunnel to the HA protects traffic to/from the Home Network.

Regarding cryptographic identifiers, the certificate of the MN is not expected to appear on the wire. In all cases, the only information one can get are associated with the MN's Home Network (HA address and possibly certificate), but nothing more specific should be disclosed. Now, considering the specific case of MN-MN communications, on the network of the initiating MN1 (the first to register with its peer), after the IKE negotiation as been performed relayed by both Home Agents, the IPsec protected Binding Update packets is emitted with the HoA of MN2 as destination (the address of the CN in previous list is the HoA of MN2). Let's consider associated SPI is 42. The packet is sent directly with the CoA of MN1 on the wire and is routed to the Home Network of the peer, before it is tunneled to it. The BA follows a reverse path but with a different SPI (say 43). After the second registration is over, the MH traffic using those SPI values (42 and 43) flows directly (remapping rules are now in place on both ends). From an eavesdropper perspective on the FL of MN1, this provides "a clue" about the association between the HoA and the CoA of the second MN2. This is introduced in [RFC4882] (Koodli, R., “IP Address Location Privacy and Mobile IPv6: Problem Statement,” May 2007.).
Note that this is the only "leaking" that happens and only on the FL of the first MN. It is no more the case on FL that are visited later. Anyway, from the perspective of an eavesdropper monitoring that, the information will be that a Mobile Node from a known Home Network (HA@) has performed IPsec communications with a MN having a known HoA (no credentials).

Author's Address

TOC

	Arnaud Ebalard
	EADS Innovation Works
	12, rue Pasteur - BP76
	Suresnes 92152
	France
Phone:	+33 1 46 97 30 28
Email:	arnaud.ebalard@eads.net