

Internet Engineering Task Force
INTERNET DRAFT
Expires in August 2004

Francis Dupont
ENST Bretagne
Wassim Haddad
Helsinki University of Technology
February 2004

How to make IPsec more mobile IPv6 friendly

<[draft-dupont-ipsec-mipv6-05.txt](#)>

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#).

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Distribution of this memo is unlimited.

Abstract

IPsec specifications [1-6] do not work well with any mobility device based on addresses [8]. Mobile IPv6 interaction with IPsec is still far from being well achieved. This is mainly due to bad interpretations of IPsec specifications. HIP (Host Identity Payload) [10] should change this regrettable situation.

This document specifies some points where improvements can be made in many current implementations, on the way of making IPsec more suitable for Mobile IPv6.

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

1. Introduction

This document assumes that the reader knows IPsec (i.e., [1-6]) but not Mobile IPv6. This section explains how Mobile IPv6 works.

In Mobile IPv6, each Mobile Node (MN) is always identified by its Home Address (H@), regardless of its current point of attachment to the Internet. While located away from its home, a MN is also associated with a Care-of Address (Co@), which provides information about the mobile node's current location. IPv6 packets from a Correspondent Node (CN) addressed to a MN's H@ are transparently routed to its Co@.

The MN has a special CN, the Home Agent (HA), which is used to intercept packets addressed to the MN's H@ on the home link and to forward them to the MN at its current Co@ through a tunnel.

End-to-end communications between a MN and a CN can use one of these three modes:

- bidirectional tunneling with the HA:
MN => HA -> CN (=> denotes an encapsulation)
CN -> HA => MN
The CN knows only the MN's H@ regardless whether the MN is mobile or not. This mode is very safe but not optimized at all.
- triangular routing:
MN ~> CN (~> denotes the use of an extension header)
CN -> HA => MN
The MN uses a Home Address Option (HAO): it puts its Co@ which is topologically correct into the source address field of the IPv6 header, and puts its H@ in the HAO.
- optimized routing:
MN ~> CN
CN ~> MN
The MN uses a HAO for packets to the CN, the CN uses a Routing Header (RH) and puts the MN's Co@ in the destination address field of the IPv6 header, and the MN's H@ in the RH. This mode raises many security concerns, mainly about the mobility signaling, but is very efficient.

These uses of HAO and RH are in fact degenerated tunnels as

shown by the Deering/Zill tunneling document [[11](#)], i.e., they can be considered as IPv6 in IPv6 tunnels where two addresses

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

in the outer and inner IPv6 headers are redundant so one instance is removed.

The association between a Co@ and the H@ is named "binding" and is cached by CNs. Bindings are managed (i.e., created, changed and deleted) by signaling messages named Binding Updates (BUs).

The term node in MN is a bit misleading: mobile routers are not considered by current Mobile IPv6 specifications and communications in this document are always end-to-end.

[2.](#) IPsec Architecture and Mobile IPv6

IPsec defines two modes, Transport and Tunnel modes.

As mobile IPv6 itself is based on real or degenerated tunneling, there are three possible basic interactions:

- Transport mode after Mobile IPv6 tunneling,
- Transport mode before Mobile IPv6 tunneling
- A combination between Tunnel mode and Mobile IPv6 tunneling.

[2.1](#) Transport Mode After Mobile IPv6

This case is defined only when Mobile IPv6 uses real tunneling, i.e., in current specifications, between the MN and its HA.

As the IPv6 header (and addresses!) viewed by IPsec is the outer one, in general this case has no interest (the MN's outer address is a transient Co@, the interesting one, the H@, is in the inner header).

[2.2](#) Transport Mode Before Mobile IPv6

In this case, the IPsec transform is applied to the payload of an ordinary packet between the MN and the CN. The MN will use its static/long term H@.

After Mobile IPv6 includes its extension header corresponding to the mode used, the following cases can be depicted:

- the bidirectional tunneling is perfectly transparent: IPsec and Mobile IPv6 do not interfere. The same consideration applies to the HA => MN tunnel.

- the triangular routing is more interesting and gives different results for the Authentication Header (AH [2]) and the Encapsulating Security Payload (ESP [3]):

- * AH authenticates both Co@ (in the IPv6 header) and the H@ (in the HAO)
- * ESP with authentication will reject fake packets because the attacker may not know the authentication shared secret.

So with authentication the only possible attack is a "Denial of Services" launched by an attacker who knows the SPI and is likely able to inject fake traffic without HAO. So this is an intrinsic IPsec thread.

*RECOMMENDATION A: Packets with a HAO matching an IPsec SA *providing authentication (i.e., AH or ESP with non-null *authentication) MUST be accepted (i.e., the HAO considered *as verifiable) and the HAO MUST be considered as verified [12] *after successful IPsec processing.

- the optimized routing is similar to the triangular routing for the MN ~> CN way and, in addition to recommendation A, the common way to verify HAO is through the "binding cache entry check". Symmetrically IPsec adds nothing to the RH check because the MN has already all important informations.
- the optimized routing between two MNs has been addressed in the Binding Update Backhauling proposal [9].

[2.3](#) Tunnel Mode not combined with Mobile IPv6

"Not combined" means the presence of two overheads, one for IPsec tunneling and another one for Mobile IPv6 extra headers. It is obvious in this case that one encapsulation provides enough addresses (two sources and two destinations) for Mobile IPv6.

*RECOMMENDATION B: IPsec in Tunnel mode and Mobile IPv6 SHOULD
*be combined in order to avoid to add their overheads.

[2.4](#) Addresses of SAs

SAs can be characterized by:

[draft-dupont-ipsec-mipv6-05.txt](#)

[Page 4]

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

- zero address (proposed inbound processing for unicast)
- one address (destination in IPsec inbound processing [[1](#)])
- two addresses (source and destination selectors [[1](#)])
- three addresses (source, destination and proxy in PF_KEY [[13](#)])
- four addresses (in Tunnel mode)

This is a bit confusing and gives security holes and/or extra checks on addresses which are highly unfriendly with Mobile IPv6.

The Transport mode is easy because there are always exactly two addresses. For instance in inbound processing, the destination address is used for the SA lookup and the source address MUST be checked ([[1](#)], section 5.2.1). So this document will assume the Tunnel mode is used.

In general, the SADB is not designed to be managed directly and/or by itself, i.e., without the SPD. Addresses are handled by the SPD with a pair of selectors characterizing the source and the destination of the traffic which receives IPsec protection. SPD entries specify the type of IPsec processing (for instance one type is the bypassing of IPsec: this is needed by IKE for its own messages [[1](#)]) and the parameters of SAs to use or to build (using SADB_ACQUIRE PF_KEY messages [[13](#)]).

According to [[1](#)] the traffic selection is divided between the SPD and the SADB (a SPD entry points to many matching SAs) but this cannot be realized using IKE so this point is very confusing, and some implementations are nearly nonconform.

IKE (and its successor(s)) is designed to build SAs per pairs, so IPsec implementations, using PF_KEY, should comply for Tunnel mode SAs with the following interpretation:

- the source and the destination addresses are plain addresses

in the general case and designate the end points of the tunnel (i.e., they are the outer header addresses).

- the inner source address is the proxy address (and exists only in the Tunnel mode). This can be different from a plain address (i.e., it can be for instance a prefix) but not in the Mobile IPv6 case. The check may be performed after each IPsec inbound processing [1] or at the SPD check (not the specified way but the final result is the same).

*RECOMMENDATION C1: The source address checked after each
*IPsec inbound processing against the SA selector MUST be
*the inner header source address.

- the selection of the traffic to be processed is handled by SPD entries. This includes the future inner addresses in outbound processing. Guidelines are to use the inbound processing rules for SADB design, the outbound processing rules for SPD design and to complete by symmetry (with the funny (?) side-effect that source and destination roles can be reversed).

[RFC 2401](#) [1] has detailed rules about the outer source address but they are commonly misunderstood: checking it gives no extra security because once an attacker can get the SPI, he can inject fake traffic too. But this check harms nearly all mobility mechanisms based on addresses, even nomadism a.k.a. the "road warrior" case.

*RECOMMENDATION C2: The outer source address in Tunnel mode
*MUST NOT be checked after or before IPsec inbound processing.

This recommendation does not apply to the SPD checking, i.e., step 4 of [RFC 2401](#) [1] [section 5.2.1](#).

This recommendation by itself does not solve the problem of the other SA of the pair: the MN may change its CoA and continue to use the SA to the CN. But the other way/SA will work only when the other SA will be updated or rebuilt with the new CoA as the destination.

BTW, [RFC 2401](#) [1] specifies IPv6 in IPv4 and IPv4 in IPv6 tunnels and these tunnels are taken into account in PF_KEY [13] so:

*RECOMMENDATION D: Dual stack (i.e., IPv4 and IPv6) IPsec implementations MUST support IPvX in IPvY Tunnel modes with any X and Y, including cases where X != Y.

[2.5 Combined Tunnel Mode with Mobile IPv6 \(Standard Case\)](#)

When IPsec in Tunnel mode is combined with Mobile IPv6, there is one encapsulation with the fixed H@ in the inner header and a transient Co@ in the outer header. Such configuration is the opposite of the common Tunnel mode usage between two security

[draft-dupont-ipsec-mipv6-05.txt](#)

[Page 6]

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

gateways.

Between two movements, the IPsec tunnels are not very special, they look like end-to-end IPsec tunnels between two peers. The only unusual detail is that the outer and inner addresses can be different (when the MN is not at home), which is an issue for IKE.

The interesting case is what happens when a Co@ changes: the MN should send a BU to the CN which, according to recommendation C, must not be filtered out because the Co@ is not the same.

*RECOMMENDATION E1: BU protected by an IPsec SA providing authentication MUST be considered as authenticated.

*RECOMMENDATION E2: In the E1 case, all BU parameters MUST be covered by the authentication. Especially when the authentication is provided by an ESP transform, the new Co@ MUST be covered by using, for instance, an alternate Co@ suboption.

The CN could ask for a proof that the new Co@ is not a fake one, i.e., the default policy may be to check the new Co@ in order to avoid reflection attacks. This check is a return routability check: the CN sends a question to the MN at its new Co@ with a predictable answer. In a thread on the mobile-ip mailing list, we proposed to reject the first BU with a "sequence number

out of the window" error.

*RECOMMENDATION E3: The CN SHOULD have the possibility to
*perform a return routability check on a new Co@ before
*recommendations E1 and E2 are applied.

As explained before, to deal with the BU is not enough for the CN ~> MN way. For instance, the Binding Acknowledgment (BA) can be protected only when the reversed SA is updated or rebuilt.

*RECOMMENDATION F: Mobility signaling and IPsec SA management
*direct cooperation SHOULD be considered (i.e., development of
*this kind of mechanisms encouraged).

[2.6](#) Combined Tunnel Mode with Mobile IPv6 (Home Agent Case)

This section does not consider traffic from the HA itself which is handled by routing optimization as for a standard CN. It is only about the MN <=> HA bidirectional tunnel.

The addresses used for this tunnel are very simple:

- on the MN side, inner header address is the H@, outer a Co@.
- on the HA side, inner header address is any valid address (unicast address when used as a source address) and the outer address is the HA address [\[7\]](#).

IPsec considerations are near the same than for standard CNs. In fact, things are simpler because one can assume the HA is never mobile. Recommendation F applies but is not useful when no IPsec SA exists, i.e., when a MN boots in visit: this will be the special case in IKE considerations (next section).

[3.](#) IKE and Mobile IPv6

There are three basic issues:

- how to handle the multiple addresses of a MN? In the phase

- one? In a phase two?
- how to establish SAs between a MN and a standard CN?
 - how to establish SAs between a MN from a foreign link and its HA the first time?

This document uses the name IKE [6] for the IPsec DOI [4] and ISAKMP [5] framework too. Some proposals for IKEv2 [13] (used as an instance of a Son-of-Ike with two phases) can be found in the [appendix B](#).

[3.1](#) IKE and Identities (Phase One)

In the phase one, identities (IDii and IDir) designate the peers, so subnet and range identities may not be used. This document assumes a phase one with digital signatures using a X.509 style of certificates, but most of the considerations applies to public key authentications too.

In a phase one, a peer is identified by its address used for the

[draft-dupont-ipsec-mipv6-05.txt](#)

[Page 8]

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

transport of IKE messages (aka the "peer address") and its identity payload. Identities, in the general meaning, may be present in certificates too but all cases are not equivalent:

- the Identity must be related to the certificate:

*RECOMMENDATION G: The Identity payload presented by the peer
*MUST be verified. For instance, when certificates are used,
*the Identity and the subject or an alternative subject of
*the certificate associated to the signature MUST match.

- if the Identity is an address, it must be the right address:

*RECOMMENDATION H: If the Identity payload presented by the
*peer is an address, it MUST be the same address than the one
*used to transport IKE messages (aka the "peer address").

- same for addresses used as (alternative) subjects:

*RECOMMENDATION I: If an address is used as the subject or as
*an alternative subject of the certificate associated to the
*signature, then the address used to transport IKE messages

* (aka the "peer address") SHOULD match the subject or an alternative subject.

"SHOULD match" means the default policy is to perform the check.

- last about Identity/address checks:

*RECOMMENDATION J: The case where the certificate associated to the signature has no address subject or alternative subject SHOULD be considered as a special case by policies. For instance, the policy MAY specify particular constraints for this case.

- of course, this can be a bit annoying for MNs which must use in some cases their Co@ for transport of IKE messages so:

*RECOMMENDATION K: The addition of a Home Address Identity, which should allow strict application of previous I and J recommendations in all MN's peer cases, SHOULD be considered in IKE.

Today the possibility to include addresses in identities is not considered to be a good idea. The [appendix B](#) about IKEv2 will

propose a very different way to solve concerns addressed by recommendations of this section (H-K).

[3.2](#) IKE and Identities (Phase Two)

In the phase two (a.k.a. quick mode) identities (IDci and IDcr) are optional and designate the policy rule (in the SPD or in the IKE software configuration) to apply:

- in Tunnel mode the peer addresses will be the outer header addresses, and identities can denote the traffic selector part of the policy rule.
- without identities the SA pairs will be applied to all traffic not matched by a more specific policy between the peers using the same addresses than in IKE messages. This is ambiguous so:

*RECOMMENDATION L1: When the phase one and phases two are

- *allowed to use different (peer) addresses to transport
*messages, identity payloads SHOULD be used in phases two.
- in Tunnel mode there is an ambiguity about the endpoint
addresses:
 - *RECOMMENDATION L2: When the phase one and phases two are
*allowed to use different addresses, the endpoint addresses
*used in a phase 2 context MUST be the (peer) addresses used
*to transport IKE messages of this phase 2.
- junk identities are not useful:
 - *RECOMMENDATION M: Identity payloads used in phase two SHOULD
*clearly denote address sets.
- IKE [6] explicitly provides a "proxy case" usable for mobility:
 - *RECOMMENDATION N: The policy MAY authorize the establishment
*of a Transport mode SA pair using an address identity payload
*which does not match the (peer) address used to transport IKE
*messages. This authorization SHOULD be based on parameters
*provided in the phase one authentication, for instance the
*phase one peer identity and certificate.

[3.3](#) IKE and Mobile IPv6 (Standard Case)

If the MN has the choice between using its H@ or a Co@ for IKE exchanges, only the first choice makes sense with a standard CN. Actually, when the initiator is the CN, it always uses the H@. Using the Co@ is more complex and should require a new phase one with each peer after a movement.

Note that the IKE software should not even notice that the node is mobile... For the same reason, the SA pairs should use the H@ as the MN address, giving an IPsec transform before Mobility case.

- *RECOMMENDATION O: With a standard CN, the MN SHOULD ignore the
*fact that it is a mobile node and SHOULD use its H@ for all IKE
*exchanges and for its own address in the SA pairs. To avoid both
*IPsec and Mobile IPv6 overheads, it SHOULD negotiate the Transport

*mode.

Transport mode was designed for end-to-end communications, IMHO this recommendation should be written with MUSTs!

[3.4](#) IKE and Mobile IPv6 (Home Agent Case)

Recommendation O does not work with the HA because, when the MN boots in visit, it can use its H@ only after processing of the first BU by the HA. This BU MUST be protected so it can not be protected by IPsec (trivial bootstrap problem).

In fact there are two possible MN - HA SA pairs:

- a SA pair for BU/BA exchange protection.
- a SA pair for the MN <=> HA tunnel.

The first SA pair is a bit hairy to establish, because the MN can only use its Co@ in some circumstances:

*RECOMMENDATION P: If BU/BA exchanges between the MN and the HA are protected by an IPsec SA pair, the establishment of this SA pair MUST be allowed using a Co@ for the transport of all IKE messages (i.e., the MN peer address is a Co@).

The detailed requirements are:

- an API should give a suitable Co@ for communications with the HA (i.e., something like getsockname() which returns

the Co@ for a connected socket to the HA address in place of the Ho@).

- phase one and phase two messages are sent using this Co@.
- the phase one identity is not an address if no transient certificate for a Co@ is available.
- the authentication with this identity must be allowed (including when recommendation J is enforced).
- until the home address identity is defined and implemented, the phase two identity must be an address identity using the H@, and this must be allowed (according to recommendation O).
- the result is a SA pair between the MN with its H@ and the HA with its HA Address. The most adequate is AH Transport mode (enough security and best efficiency).

This SA pair establishment stresses the issue of relative lifetimes of the phase one and the SA pair so:

*RECOMMENDATION Q: IKE implementations MUST support lifetimes
*for the phase one, which are far longer or far shorter than
*the lifetime of SA pairs established by phases two.

and with very long phase one lifetimes:

*RECOMMENDATION R: IKE implementations SHOULD be able to lookup
*a still valid phase one state from a phase two message using
*different (peer) addresses for transport. For instance using the
*ISAKMP SA SPI a.k.a. cookies [5].

The SA pair for the tunnel is more easy: the only problem is about policies:

- A solution is to dynamically create the proper policy from mobility information (i.e., BUs) and to establish the SA pair described in [section 2.6](#) (combined Tunnel mode with HA). One can make things a bit faster reusing the phase one (c.f. recommendations R and L2).
- Another solution is to create a SA pair using only the MN's H@ (this can be done as soon as the first BU is processed because the HA can use the standard routing optimization mode for its own traffic. In fact this is the default behavior), and to use a to-be-defined direct cooperation mechanism between IPsec and mobility to update the outer MN address in the SA pair (a good use of the HIP readdress [10]).

[4.](#) Security Considerations

At the exception of recommendations F and K, all recommendations made in this document are about interpretation of IPsec specification details. In fact, we are convinced these recommendations shall improve the security of both IPsec and Mobile IPv6.

[5.](#) Acknowledgments

Some of the MN - HA ideas were developed in the authentication vs. authorization brainstorming, for instance the home address identity (unfortunately I don't remember who proposed this).

Of course the current terrible interaction between IPsec and Mobile IPv6 was and still is discussed in the mobile-ip WG list and from time to time in the ipsec WG list too. So many thanks to the little number of persons who participate to both lists.

The return routability check for new CoA was proposed by Alper Yegin and makes IPsec a very good candidate in the MN - CN case when it is applicable.

I finish with authors of "open source" IKE implementations, particularly Shoichi Sakane who has written the IPsec implementation (including an IKE daemon, racoon) I use.

6. Normative References

[1] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998.

[2] S. Kent, R. Atkinson, "IP Authentication Header", [RFC 2402](#), November 1998.

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

[4] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", [RFC 2407](#), November 1998.

[5] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)",

[draft-dupont-ipsec-mipv6-05.txt](#)

[Page 13]

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

[RFC 2408](#), November 1998.

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

[7] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", [draft-ietf-mobileip-ipv6-24.txt](#), June 2003.

7. Informative References

- [8] F. Dupont, "Mobility-aware IPsec ESP tunnels", [draft-dupont-movesptun-00.txt](#), February 2001.
- [9] W. Haddad and all, "Binding Update Backhauling", [draft-haddad-mip6-bub-01.txt](#), February 2004.
- [10] R. Moskowitz and all, "Host Identity Payload And Protocol", [draft-moskowitz-hip-09.txt](#), February 2004.
- [11] S. Deering, B. Zill, "Redundant Address Deletion when Encapsulating IPv6 in IPv6", [draft-deering-ipv6-encap-addr-deletion-00.txt](#), November 2001.
- [12] C. Perkins, "[mobile-ip] A new proposal for handling Home Address destination options", <http://playground.sun.com/mobile-ip/>, Message-ID: <3C6C7780.4CFAA7B4@iprg.nokia.com>, February 2002.
- [13] D. McDonald, C. Metz, B. Phan, "PF_KEY Key Management API, Version 2", [RFC 2367](#), July 1998.

8. References for Appendixes

- [14] C. Kaufman, ed., "Proposal for the IKEv2 Protocol", [draft-ietf-ipsec-ikev2-12.txt](#), January 2004.
- [15] B. Korver, E. Rescorla, "The Internet IP Security PKI Profile of ISAKMP and PKIX", [draft-ietf-ipsec-pki-profile-03.txt](#), July 2003.
- [16] P. Hoffman, "Adding revised identities to IKEv2", <http://www.vpnc.org/ietf-ipsec/>, Message-Id: <p05200f06b9edf48ac57b@[165.227.249.18]>, November 2002.

[draft-dupont-ipsec-mipv6-05.txt](#)

[Page 14]

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

- [17] M. Kaat, "Overview of 1999 IAB Network Layer Workshop", [RFC 2956](#), October 2000.
- [18] F. Dupont, J.-J. Bernard, "Transient pseudo-NAT attacks

or how NATs are even more evil than you believed",
[draft-dupont-transient-pseudonat-02.txt](#), October 2003.

[19] S. Deering and all, "IPv6 Scoped Address Architecture",
[draft-ietf-ipv6-scoping-arch-00.txt](#), June 2003.

[20] Franck Le and all, "Mobile IPv6 Authentication, Authorization,
and Accounting Requirements",
[draft-le-aaa-mipv6-requirements-02.txt](#), April 2003.

9. Author's Address

Francis Dupont
ENST Bretagne
Campus de Rennes
2, rue de la Chataigneraie
CS 17607
35576 Cesson-Sevigne Cedex
FRANCE
Fax: +33 2 99 12 70 30
EMail: Francis.Dupont@enst-bretagne.fr

Wassim Haddad
Helsinki University of Technology
Theoretical Computer Science Laboratory
PO BOX 9201
HUT 02015
Finland
EMail: whaddad@tcs.hut.fi

10. Changes from Previous Drafts

Addition of recommendation E3 about return routability check
for new Co@.

Addition of [Appendix A](#) (list of recommendations), B (proposals
for IKEv2), C (return routability) and D (scoped addresses).

Introduction of the "peer address" term.

[draft-dupont-ipsec-mipv6-05.txt](#)

[Page 15]

New appendix about mobile IPsec VPN.

Appendix A: List of Recommendations

- A: Packets with a HAO matching an IPsec SA providing authentication (i.e., AH or ESP with non-null authentication) MUST be accepted (i.e., the HAO considered as verifiable) and the HAO MUST be considered as verified [12] after successful IPsec processing.
- B: IPsec in Tunnel mode and Mobile IPv6 SHOULD be combined in order to avoid to add their overheads.
- C1: The source address checked after each IPsec inbound processing against the SA selector MUST be the inner header source address.
- C2: The outer source address in Tunnel mode MUST NOT be checked after or before IPsec inbound processing.
- D: Dual stack (i.e., IPv4 and IPv6) IPsec implementations MUST support IPvX in IPvY Tunnel modes with any X and Y, including cases where $X \neq Y$.
- E1: BU protected by an IPsec SA providing authentication MUST be considered as authenticated.
- E2: In the E1 case, all BU parameters MUST be covered by the authentication. Specially when the authentication is provided by an ESP transform, the new Co@ MUST be covered by using, for instance, an alternate Co@ suboption.
- E3: The CN SHOULD have the possibility to perform a return routability check on a new Co@ before recommendations E1 and E2 are applied.
- F: Mobility signaling and IPsec SA management direct cooperation SHOULD be considered (i.e., development of this kind of mechanisms encouraged).
- G: The Identity payload presented by the peer MUST be verified. For instance, when certificates are used, the Identity and the subject or an alternative subject of the certificate associated to the signature MUST match.

- H: If the Identity payload presented by the peer is an address, it MUST be the same address than the one used to transport IKE messages (aka the "peer address").
- I: If an address is used as the subject or an alternative subject of the certificate associated to the signature, then the address used to transport IKE messages (aka the "peer address") SHOULD match the subject or an alternative subject.
- J: The case where the certificate associated to the signature has no address subject or alternative subject SHOULD be considered as a special case by policies. For instance, the policy MAY specify particular constraints for this case.
- K: The addition of a Home Address Identity, which should allow strict application of previous I and J recommendations in all MN's peer cases, SHOULD be considered in IKE.
- L1: When the phase one and phases two are allowed to use different (peer) addresses to transport messages, identity payloads SHOULD be used in phases two.
- L2: When the phase one and phases two are allowed to use different addresses, the endpoint addresses used in a phase 2 context MUST be the (peer) addresses used to transport IKE messages of this phase 2.
- M: Identity payloads used in phase two SHOULD denote clearly address sets.
- N: The policy MAY authorize the establishment of a Transport mode SA pair using an address identity payload which does not match the (peer) address used to transport IKE messages. This authorization SHOULD be based on parameters provided in the phase one authentication, for instance the phase one peer identity and certificate.
- O: With a standard CN, the MN SHOULD ignore the fact that it is a mobile node and SHOULD use its H@ for all IKE exchanges and for its own address in the SA pairs. To avoid both IPsec and Mobile IPv6 overheads, it SHOULD negotiate the Transport mode.
- P: If BU/BA exchanges between the MN and the HA are protected by an IPsec SA pair, the establishment of this SA pair MUST be allowed using a Co@ for the transport of all IKE messages (i.e.,

the MN peer address is a Co@).

Q: IKE implementations MUST support lifetimes for the phase one which are far longer or far shorter than the lifetime of SA pairs established by phases two.

R: IKE implementations SHOULD be able to lookup still valid phase one state from a phase two message using different (peer) addresses for transport. For instance using the ISAKMP SA SPI a.k.a. cookies [5].

Appendix B: Proposals for IKEv2

Many recommendations are directly applicable to IKEv2 [14]:

- recommendations G, O, P apply without modifications.
- recommendations L1, L2 and N applies to traffic selectors in place of phase two identities.
- recommendation M is integrated in IKEv2.
- recommendation R is partially integrated in section 2.6 of [14], but we propose to make very clear the IKE-SA lookup MUST be done using the cookies as a SPI *only*. Note that IKEv2 guarantees the uniqueness of these "SPIs".

[15] introduces the term "peer addresses" for the addresses used for the transport of IKE messages and includes the recommendations G, H and I. [16] is not directly applicable to IKEv2 but [16] (not yet included in the IKEv2 draft) proposes a new form of identities without any kind of binding to addresses.

In IKEv2 the phase one SA is named the IKE SA and when it is deleted all the IPsec SAs it negotiated have to be deleted too (so the recommendation Q does not stand). The idea is to solve the dead peer detection issue by keepalives over the IKE SA.

*PROPOSAL 1: IKEv2 implementations MUST lookup IKE-SA using *only the SPI at the exclusion of peer addresses.

Identities should not include addresses as recommended in [16] so recommendations H to K are obsolete in the IKEv2 context. (this is a call to adopt [15] ASAP)

*PROPOSAL 2: IKEv2 identity payloads MUST only use abstract *identities as recommended in [17] by the IAB and proposed by [15]. But this and the [section 4.11](#) "Address and Port Agility" of [13]

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

remove any check of peer addresses which are still part of established SAs, opening the door to attacks as described in [18]. But mobility really needs address agility so:

*PROPOSAL 3: The [section 4.11](#) should specify full address agility.

The first counter-measure against abuse of this address agility is to protect the integrity of transport headers. The new notifications NAT-DETECTION-SOURCE-IP and NAT-DETECTION-DESTINATION-IP are the beginning of a solution.

*PROPOSAL 4: IKEv2 MUST provide a way to protect the integrity of transport parameters (peer addresses, ports and protocol).

*PROPOSAL 5: The default policy SHOULD be the protection of the integrity of transport parameters for IPv6.

These proposals defeat en-route modifications of messages, i.e., fulfill some mobility requirements, but not all of them because these proposals give no proof about the real origin of messages, i.e., one should trust its peer. The solution is of course a simple return routability check, and IKEv2 already uses this kind of mechanisms in the "Responder under attack" case (IKE_SA_init_reject).

*PROPOSAL 6: A mechanism MUST be provided in order to make return routability checks available on peer address changes.

*PROPOSAL 7: The default policy SHOULD be to perform return routability checks on peer address changes.

Now that mobility can be securely handled (this is not the case for NAT traversal but we believe this issue can not be solved, c.f. [17]), we can look for some dedicated improvements. The first special case to be dealt with is the MN - HA SA pair to protect the BU/BA exchange a.k.a. the "home registration".

*PROPOSAL 8: When the policy authorizes it, a traffic selector in Transport mode MAY override peer addresses as SA selectors.

(this is a reformulation of recommendations N and P.)

The other item is to instantiate the recommendation F:

INTERNET-DRAFT

IPsec more MIPv6 friendly

February 2004

*PROPOSAL 9: A new mechanism MUST be defined for the update
*of the peer address in the SA pair (the source outer address of
*the inbound SA and the destination outer address of the outbound
*SA) without mandatory rekeying.

Appendix C: Return Routability

The proposed return routability check assumes these properties:

- a secret is shared with the peer, i.e., there is a proof that the received packets are from the peer.
- an anti-replay mechanism proves the received packets are fresh.

If the exchange involved some hard state change (for instance the proposal 9), a sequencing mechanism should be provided too.

The return routability check does not give a proof that the peer is at the given address, it only proves the peer is on the path. For more details about return routability check theory, please refer to [\[7\]](#).

Appendix D: Scoped Addresses

This topic is not really a Mobile IPv6 one, but in practice the "mobile VPN" case there is a heavy usage of limited scope or private addresses.

The issue is that addresses carried in identity or traffic selector payloads are not clothed with zone identifiers. Only the peer addresses used to transport messages have an indirect indication of their zones.

The IPv6 scoped address architecture [\[19\]](#) gives the properties of zones: at a given scope, zones form a partition, i.e., an interface belongs to one and only one zone. They have an inclusion property too, i.e., a zone of a given scope is fully included into a zone of any higher scope. This gives an inheritance property which is safe when it is used in

the proper way: to establish SAs with global addresses with IKE running over link-local addresses is safe, the opposite is not.

*RULE: The default policy SHOULD accept scoped addresses as

*selectors of SAs only when they are established using peer
*addresses (for the transport of IKE/IKEv2/etc messages) which
*are in fully included zones.

Appendix E: mobile IPsec VPN

Mobile IPsec Virtual Private Networks (VPNs) provides the same kind of functionality than mobile IP: the VPN client (the Mobile Node in the mobility context) opens an ESP tunnel with a Security Gateway (the equivalent of a Home Agent) located in the home site.

Even if the style of mobile IPsec VPNs are more Mobile IPv6 than Mobile IPv4 (there is no equivalent of Foreign Agents for instance), they can be used for the two versions of IP so this appendix is about both.

Current mobile IPsec VPNs have no Security Gateway detection, support for multiple inner addresses, prefix discovery, etc, but they can be connected to a remote network access control with an optional address allocation. Today they have no support for an extended AAA system where the AAA infrastructure connects the local and remote network access control with some assistance to the initial security setup (via credentials and/or piggy-backing of IKE initial exchanges [20]).

The layout of data packets of mobile IPsec VPNs are exactly the same than for Mobile IPv6 with an ESP protected MN-HA bidirectional tunnel (the outer header client address is a Care-of Address, the inner one is the Home Address) at one exception: in Mobile IPv6 the Home Agent is a correspondent node for its own address, for instance the Home Agent sends genuine packets to the Mobile Node using a Routing Header, not through the tunnel. If the corresponding rule of [7] ([section 9.3.2](#) Sending Packets to a Mobile Node) is applied only to Mobile IPv6 signaling packets, mobile IPsec VPNs and Mobile IPv6 are indistinguishable.

So mobile IPsec VPNs are a good replacement for unoptimized Mobile IPv6 or for Mobile IPv4 with secure reverse tunneling. Movements can be handled by peer address update mechanisms, including rekeying.