MIP6 Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 26, 2009

F. Dupont
ISC
J-M. Combes
Orange Labs R&D
August 25, 2008

Using IPsec between Mobile and Correspondent IPv6 Nodes
draft-ietf-mip6-cn-ipsec-08.txt

Status of this Memo

Abstract

Mobile IPv6 uses IPsec to protect signaling between the Mobile Node and the Home Agent. This document defines how IPsec can be used between the Mobile Node and Correspondent Nodes for Home Address Option validation and protection of mobility signaling for Route Optimization. The configuration details for IPsec and IKE are also provided.

1. Introduction

Mobile IPv6 documents [RFC3775][RFC3776][RFC4877] specify IPsec

[RFC4301] for the protection of the signaling between the Mobile Node (MN) and its Home Agent (HA), and the return routability procedure between the Mobile Node and its Correspondent Nodes (CN) for Route Optimization. This document defines an alternative mechanism for Mobile IPv6 route optimization based on strong authentication and IPsec.

It specifies which IPsec configurations can be useful in a Mobile IPv6 context and how they can validate Home Address Options (enabling triangular routing) and protect mobility signaling (enabling Route Optimization). It gives detailed IKE [RFC2409][RFC4306] configuration guidelines for common cases.

Note when the design goal of the return routability procedure was to be "not worse than the current Internet", the design goal of this document is "not worse than deployed IPsec".

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].

IKE terminology is copied from IKEv2 [RFC4306] [IKEv2bis].

2. Applicability

The purpose of this document is not to replace the return routability procedure, specified in [RFC3775], by the use of IPsec/IKE. It is unrealistic to expect credentials to be available today for strong authentication between any pair of Internet nodes.

The idea is to enable the use of the superior security provided by IPsec when it is already in use (i.e., comes at no extra cost), when obstacles (i.e., authentication) to its use no more stand in the way, or simply when it can be considered as highly desirable.

This mechanism should only be turned on by explicit configuration between specific peers. This explicit configuration involves turning on the mechanism specified in this document and turning off the Mobile IPv6 Return Routability mechanism. It does not support automatic capability negotiation at this time.

It is expected that certificate enrollment supports the inclusion of the Home Address of a node in the node certificate when the Home Address is known in time.

It is REQUIRED that nodes conforming to this specification implement the base Mobile IPv6 as specified in RFC 3775 [RFC3775] (either in

Mobile or Correspondent Node role or in both).

3. IPsec in a Mobile IPv6 context

This document considers only suitable IPsec Security Associations, i.e., anything which does not fulfill the following requirements is out of scope:

- IPsec Security Association pairs MUST be between the Mobile Node and one of its Correspondent Nodes.
- origin authentication, payload integrity and anti-replay services MUST be enabled.
- the Traffic Selectors MUST match exclusively the Home Address of the Mobile Node and an address of the Correspondent Node (the address used for communication between peers).
- IPsec transport mode MUST be used.
- for Route Optimization, the Mobility Header "upper protocol" with at least Binding Update (BU, from the MN) and Binding Acknowledgment (BA, from the CN) message types MUST be accepted by the Traffic Selectors.

The purpose of the first three requirements is to allow IPsec to provide a proof of origin. The third one enforces the use of the proper Home Address.

4. Home Address Option validation

This document amends the Mobile IPv6 [RFC3775] section 9.3.1 by adding a second way (other than Binding Cache Entry check) to provide Home Address Option validation.

When a packet carrying a Home Address Option is protected by a suitable IPsec Security Association, the Home Address Option SHOULD be considered valid.

A way to implement this is to mark the Home Address Option as "to be validated" when it is processed. When the upper protocol is reached, in order either:

- an IPsec header was processed according to [RFC4301] section 5.2 with a suitable IPsec Security Association, or
- a Binding Cache Entry check is successfully performed, or
- the packet contains a Binding Update, or
- the packet MUST be dropped.

By just setting up an IPsec SA with the CN, the MN is able to send packets directly to the CN, i.e., triangular routing is enabled. The CN does the Home Address Option validation by successful IPsec

processing of the packet. The Care-of Address in the source address field of the IPv6 header is not used by IPsec at all as the IPsec policy checks happen against the Home Address. The CN continues to send the packets via the home network until a Binding Update is processed.

5. Route Optimization

A suitable IPsec Security Association can protect Binding Updates and Acknowledgments. In Binding Updates the new requirements are:

- Nonce Indices and Binding Authorization Data options SHOULD NOT be sent by the Mobile Node and MUST be ignored by the Correspondent Node.
- when an Alternate Care-of Address option is present, the alternate Care-of Address MUST match the source address in the IP header or the Home Address itself. Any Binding Update which does not fulfill this requirement MUST be rejected.

In Binding Acknowledgments the new requirement is:

- Binding Authorization Data option SHOULD NOT be sent by the Correspondent Node and MUST be ignored by the Mobile Node.

The use of the K (Key Management Mobility Capability) bit with Correspondent Nodes is not defined. This bit is always set to zero on sending a Binding Update or Binding Acknowledgment, and ignored on receipt.

Note that a relatively long lifetime compatible with the IPsec policy (i.e., by default up to the IPsec Security Association lifetime) MAY be used with correspondent registrations, in contrast to the short lifetime required by standard RFC 3775 mechanisms.

6. IKE configurations

6.1. Introduction

This section should be understandable (so applicable) from both the mobility and IPsec/IKE points of view:

- IKE is an application like any other, mobility is not directly visible by IKE. This is different and simpler than the Mobile Node - Home Agent [RFC3776] [RFC4877] situation.
- the key point in the use of IKE by the mobility is to enforce the Section 3 requirements.

In particular, it is REQUIRED the Home Address of the Mobile Node matches exclusively the address of the Mobile Node in the Traffic

Selector. So this section can use one of these two terms to indicate this address.

6.2. Requirements

Addresses IKE runs over (aka. the peer addresses) are the addresses seen at the transport or application layer. With this definition, IKE MUST be run over the Home Address for the Mobile Node side when the Home Address is usable. The case where the Home Address in unusable is the subject of Appendix A.

The Home Address MAY be used in (phase 1) Mobile Node Identification payloads. But this does not work well with dynamic Home Addresses, so when it is acceptable by the Correspondent Node policy, name based Identification (i.e., of type ID_FQDN or ID_RFC822_ADDR, [RFC4306] section 3.5) payloads SHOULD be used by the Mobile Node.

Note the PKI profile for IKE [RFC4945] applies so when the Mobile Node uses an Identification payload with the ID_IPV6_ADDR type, the Mobile Node MUST put the Home Address in it and the Correspondent Node MUST verify that the address in the Identification payload will be the Home Address.

6.3. Authorization

The IPsec/IKE configuration MUST constraint the authorized traffic, in particular the Child SA Authorization Data [RFC4301] [IKEv2bis] SHOULD authorize the Home Addresses per Mobile Node and per Address. This requirement applies to the whole IPsec/IKE configuration, not only the mobility related part.

The Correspondent Node MUST verify the authorization of the Home Address, and it MUST refuse to established IPsec SAs with a not-authorized Home Address. For instance, this check is REQUIRED when the Home Address can be the address in an iPAddress field in the SubjectAltName extension [RFC3280] of the Mobile Node certificate; or when the Home Address can be the address used to lookup a pre-shared key.

Dynamically assigned Home Addresses are not known a priori so it is not possible to individually authorize them. In this case the authorization SHOULD be done using the ranges of the possible dynamically assigned Home Addresses.

7. IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

8. Security Considerations

The Mobile IPv6 Route Optimization security design background document [RFC4225] describes the unauthorized creation of Binding Cache entries as the main avenue of attack. The authentication and authorization of the Mobile Node provided by IPsec/IKE is a strong defense against this threat.

Where the means to create suitable IPsec security associations exist, this mechanism provides origin authentication, integrity protection, replay protection and optional confidentiality services for the Mobile IPv6 signaling. This improves the security over RFC 3775 route optimization, as the signaling packets in the latter are vulnerable to man-in-the-middle attacks. The implications of this vulnerability are that an attacker performing the man-in-the-middle attack can have access to the security material needed to create MIPv6 signaling instead of the Mobile Node. On the other hand, an attacker in the same position is also capable of seeing all the payload packets and could launch other attacks with similar implications. For instance, such an attacker could see or modify the contents of payload packets not protected with end-to-end security and cause denial-of-service for others. However, the RFC 3775 mechanism allows such attacks in a short time window even after the attacker is no longer in a position to see the payload packets themselves. The mechanism defined in this specification removes this vulnerability.

However, unlike RFC 3775 this mechanism should only be used when the correspondent node has good reason to trust the actions of the mobile node. In particular, the correspondent node needs to be certain that the mobile node will not launch flooding attacks against a third party as described in [RFC4225]. Without such trust the only protection comes from the application of ingress filtering in the network where the attacker resides. However, at the moment ingress filtering has not been universally deployed. This mechanism is vulnerable to flooding attacks as it does not verify the validity of a claimed new care-of address. Note, however, the following:

- The attacker has to be the Mobile Node itself, i.e., the IPsec/IKE peer, which is supposed to be the subject of a minimal level of trust.
- The attack can be easily traced back to the Mobile Node.

In order to avoid granting extra privileges by a side effect, the application of this mechanism must not lead to allowing any new,

previously unauthorized traffic to flow between the peers beyond mobility signaling with the Mobility Header (MH) protocol. The IPsec peer policy MAY also restrict IPsec Security Associations to the protection of Mobile IPv6 signaling, i.e., restrict the Traffic Selectors to MH with at least Binding Update and Binding Acknowledgment message types.

Although the protection of static addresses is not mandatory in IPsec or Home Addresses do not introduce a specific issue, this document requires authorized Home Addresses, and recommends individual or range authorization according to what is possible. This protects a Mobile Node using a static so likely known Home Address against the theft of its Home Address, both when the security associations are established and without limitations when they are used. Dynamic addresses are not protected against spoofing but the spoofing is limited to the dynamic address ranges, i.e., Mobile Nodes using dynamically assigned Home Addresses can be attacked between them. Finally the authorization requirement applies to the whole configuration so mobility is protected against other usages of IPsec.

9. Acknowledgments

The authors would like to thank many people for believing in IPsec as a right way to secure Mobile IPv6. Special thanks to Wassim Haddad and Claude Castelluccia for keeping our attention to special cases where Home Addresses are derived from public keys. Thanks to Mohan Parthasarathy for the peer address clarification and to Jari Arkko for the time he spent to improve the document.

10. Possible enhancements

A number of potential enhancements of this method are possible, including, for instance, various mechanisms for verification of Care-of Addresses or use of addresses bound to keys. [RFC4651] describes many proposals for the general Route Optimization problem.

[I-D.dupont-mipv6-rrcookie] is an alternate approach to testing Care-of Addresses.

When the Home Address is bound to a public key, for instance when the Home Address is a Cryptographically Generated Address [RFC3972], [I-D.laganier-ike-ipv6-cga] describes an alternative approach to the use of strong authentication.

11. Changes from the previous version

To be removed prior to publication as an RFC.

None.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997.

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

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

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

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

[RFC4945] Korver, B., "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX", RFC 4945, August 2007.

12.2. Informative References

[I-D.dupont-mipv6-rrcookie]
Dupont, F. and J-M. Combes, "Care-of Address Test for MIPv6 using a State Cookie", draft-dupont-mipv6-rrcookie-05.txt (work in progress),

November 2007.

[I-D.laganier-ike-ipv6-cga]
Laganier, J. and G. Montenegro, "Using IKE with IPv6 Cryptographically Generated Addresses", draft-laganier-ike-ipv6-cga-02.txt (work in progress), July 2007.

[IKEv2bis]
Kaufman, C., Hoffman, P., and P. Eronen, "Internet Key Exchange Protocol: IKEv2", draft-hoffman-ikev2bis-02.txt (work in progress), November 2007.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[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.

[RFC4651] Vogt, C. and J. Arkko, "A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization", RFC 4651, February 2007.

[RFC4843] Nikander, P., Laganier, J., and F. Dupont, "An IPv6 Prefix for Overlay Routable Cryptographic Hash Identifiers (ORCHID)", RFC 4843, April 2007.

Appendix A. IKE running over a Care-of Address

In special circumstances where the Home Address can be unusable, as when the Home Address is ORCHID [RFC4843] based and not routable, IKE must be run over a Care-of Address but this has many known drawbacks:

- a Care-of Address can not be used for authentication nor authorization.
- Security Associations do not survive handoffs.
- the establishment of transport mode IPsec Security Association using the Home Address as the Mobile Node Traffic Selector raises a policy / authorization issue as IKE runs over another address.

Authors' Addresses

Francis Dupont
ISC

Email: Francis.Dupont@fdupont.fr

Jean-Michel Combes
Orange Labs R&D
38 rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
France

Email: jeanmichel.combes@gmail.com

Full Copyright Statement

Intellectual Property