Francis Dupont
GET/ENST Bretagne
Jean-Michel Combes
France Telecom R&D
June 2004

Using IPsec between Mobile and Correspondent IPv6 Nodes

<draft-dupont-mipv6-cn-ipsec-01.txt>

Status of this Memo

Abstract

Mobile IPv6 [1] uses IPsec [2] to protect signaling between the mobile node and the home agent [3]. This document defines how IPsec could be used between the mobile node and correspondent nodes, including home address option validation (aka. triangular routing), protection of mobility signaling for routing optimization and suitable configurations.

1. Introduction

Mobile IPv6 documents [1,3] specifies IPsec 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 routing optimization. But any stronger mechanism (i.e., more secure than the return routability procedure) MAY be used, including of course IPsec.

This document 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 routing optimization). It gives detailed IKE [4,5] configuration guidelines for common cases. An annex proposes an extension of mobility signaling for the safe support of alternate care-of addresses.

This document uses the "MUST", "SHOULD", "MAY", ..., key words according to [6]. IKE terminology is copied from IKEv2 [5].

2, 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.
- authentication, integrity and anti-replay services MUST be selected.
- 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).
- the transport mode MUST be used.
- for routing optimization, the mobility header "upper protocol" with at least binding update (BU) and acknowledgment (BA) message type MUST be accepted by the traffic selectors.

The purpose of the first three requirements is to allow using IPsec as a proof of origin.

3. Home address option validation

This document amends the Mobile IPv6 [1] 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 as validated.

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 [2] section 5.2.1 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.

Note this enables triangular routing from any unicast routable care-of address, i.e., half optimization without any mobility signaling.

4. Routing Optimization

A suitable IPsec security association can protect binding updates and acknowledgments. In binding updates the new requirements are:

- the H (home registration) and K (key management mobility capability) bits MUST be cleared.
- 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 and the Annex is not in use, 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.
- as ESP can only protect the payload, an alternate care-of address option MUST be used in conjunction with ESP (cf [1] section 11.7.1).

In binding acknowledgments the new requirements are:

- the K (key management mobility capability) bit MUST be cleared.
- Binding authorization data option SHOULD NOT be sent by the correspondent node and MUST be ignored by the mobile node.
- "long" lifetime compatible with the IPsec policy (i.e., by default up to the IPsec security association lifetime) MAY be granted.

As explained in [9], ingress filtering either is not used and bombing attacks are possible without the "help" of any Mobile IPv6 mechanism, or is used and provides protection against fake care-of addresses from a rogue mobile node. So the only constraint is to accept real alternate care-of addresses only with the Annex procedure.

5. IKE configurations

This document considers only IKE where it is used for mobility purpose. Peer addresses (addresses IKE runs over) are the addresses seen at the transport or application layers, i.e., when the mobile node uses its home address as the source of an IKE message the source address in the IP header can (should!) be a care-of address.

IKE MUST be run over the home address for the mobile node side when the home address is usable. In special circumstances where the home address can be unsable, 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.

The home address MAY be used in (phase 1) mobile node Identity payload. But this does not work well with dynamic home addresses, so when it is acceptable by the correspondent node policy, name based Identity (i.e., of type ID_FQDN or ID_RFC822_ADDR, [5] section 3.5) payloads SHOULD be used by the mobile node

When the home address is bound to a public key, for instance when the home address is a Cryptographically Generated Addresses (CGA) [10], the strong authentication MAY be replaced by an address ownership proof. In this case the public key MAY be transported by IKE from the mobile node to the correspondent node, for instance in a Certificate payload of type 11 ([5] section 3.6). Auxiliary parameters MAY be transported in an Identity payload of type ID_KEY_ID...

The IKE peer policy MAY restrict IPsec security associations to the protection of Mobile IPv6 signaling, i.e., restrict the traffic selectors to the mobility header "upper protocol" with at least binding update and acknowledgment message types. This SHOULD be the default policy when authentication or authorization can be considered as weak, for instance when the previous paragraph is applied.

6. Security Considerations

IPsec is far more secure than the return routability procedure, thus it should be used where it is applicable. So this document could increase at least the overall security of Mobile IPv6. Note that some operators can not propose Mobile IPv6 based services knowing that the Mobile IPv6 security is based on assumptions.

Two points are worthy of special considerations:

- no care-of address test is required when ingress filtering can reject fake care-of addresses from a rogue mobile node but a correspondent node can use the Annex procedure to get extra insurance as well as support real alternate care-of addresses.
- in order to avoid granting any extra privilege by a side effect of using IPsec, the peers (i.e., the mobile and correspondent nodes) may restrict the traffic selectors to the protection of mobility signaling only. This should be applied to any dubious cases, including by default when security administration is known to be too light.

7. 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 the Mobile IPv6 IETF working group for discussions about the third party bombing issue, including for no convincing arguments in favor of a requirement for the care-of address test. No thanks to router vendors who do not support ingress filtering with reasonable performance on some models, and to Internet service provider managers who could enable ingress filtering but did not.

8. Normative References

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

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

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

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

[5] C. Kaufman, ed., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-14.txt, May 2004.

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

[7] R. Stewart & all, "Stream Control Transmission Protocol", RFC 2960, October 2000.

[8] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, March 1997.

9. Informative References

[9] F. Dupont, "A note about 3rd party bombing in Mobile IPv6", draft-dupont-mipv6-3bombing-00.txt, February 2004.

[10] T. Aura, "Cryptographically Generated Addresses (CGA)", draft-ietf-send-cga-06.txt, April 2004.

10. Authors' Addresses

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

Jean-Michel Combes
France Telecom R&D - DTL/SSR
38/40, rue du General Leclerc
92794 Issy-les-Moulineaux Cedex 9
FRANCE
Fax: +33 1 45 29 65 19
EMail: jeanmichel.combes@francetelecom.com

11. Changes from the previous version

Front IPR statement (cf new I-D guidelines).
Peer address clarification (thanks to Mohan Parthasarathy).
Change SHOULD/MAY to MUST/MUST for mobile node peer address.
Reference updates.

A1. Signaling extension for alternate care-of address support

This Annex defines a procedure which performs a "care-of address test". This procedure MAY be used in order to check whether the mobile node can really receive packets sent to the care-of address of a new binding update. It SHOULD NOT be used for entry deletion, i.e., when the care-of address is the home address. It MUST be used for real alternate care-of address, i.e., when the address carried by an alternate care-of address option is not the source address of the IP header nor the home address of the mobile node (following the recommendation of [9]).

The procedure is based on the state cookie used in SCTP [7] which can be found again in IKEv2 proposal [5]. The binding update is in a first time (1) rejected by a binding acknowledgment with a new dedicated status and a cookie option sent to the tested care-of address. Unpon the reception (2) of this binding acknowledgment, the mobile node retransmits (3) the binding update with the exact received cookie placed in a cookie option. When the correspondent node receives (4) the augmented binding update, it can check by recomputing the cookie and comparing it to the cookie option that the binding update is from the same mobile node and for the same care-of address (so it can infer the mobile node is reachable at this care-of address, i.e., a "care-of address test" has been successfully performed).

The cookie MUST reflect the mobile node identity or the binding cache entry or an equivalent, and MUST reflect the tested care-of address. It MUST not be easy to infer by the mobile node, including with the knowledge of previous cookies from the same node.

Two methods of generating cookies are proposed, the first one uses a secret per binding cache entry, the second uses a global secret.
The first method uses in sequence:

- a 16 bit timestamp on when the cookie is created
- the tested care-of address
- the truncated HMAC [8] keyed by the binding cache entry secret key of the preceding two fields and the correspondent address.

The second method uses in sequence:

- a 16 bit timestamp on when the cookie is created
- the tested care-of address
- the truncated HMAC [8] keyed by the global secret key of the preceding two fields, the home address and the correspondent address.

The secret key SHOULD be random or pseudo-random and SHOULD be changed reasonably frequently. The timestamp MAY be used to determine which key was used. The HMAC has to be truncated in order to keep the cookie option length less than the maximum, the higher 96 bits of the HMAC should be enough.

The last point is what to do waiting the retransmitted and augmented binding update. Possibilities are:

- apply the binding update with the new care-of address. This defeats the purpose of the care-of address test so it SHOULD NOT be done, and it MUST NOT be done for a real alternate care-of address.
- keep the previous care-of address. As it is not possible to know whether the previous care-of address is usable, i.e., whether the mobile node is still reachable at this previous care-of address, the default policy SHOULD NOT be to keep the previous care-of address. The correspondent node MAY keep the previous care-of address in special cases where this is known to be the best solution.
- temporarily disable the binding cache entry, i.e., by using the home address for communication to the mobile node until another binding update is received. This SHOULD be the default policy.

A2. IANA Considerations

This Annex requires:

- a new status for binding acknowledgment.
- a new option for mobility messages used in binding update and acknowledgment messages.