Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: June 21, 2008

S. Decugis
University of Tokyo

December 19, 2007

Key Management Mobility Capability (K) flag in Mobile IPv6 BU/BA messages.
draft-sdecugis-mextkbitissues-00

Status of this Memo

Copyright Notice

Abstract

Mobile IPv6 specification (RFC 3775) introduces a flag called "Key Management Mobility Capability (K)" to use during the home registration procedure (BU/BA exchange.) This document describes the sequences of events that occur when this flag is not used by the implementation. It also highlights the requirements that this flag

puts on the interface between the MIPv6 entity and the IKE entity.

Table of Contents

1. Introduction

This introduction presents briefly the Mobile IPv6 dynamic keying, and the exact meaning of the 'K' flag in BU/BA messages. Previous knowledge of the Mobile IPv6 RFC 3775 [RFC3775], IPsec RFC 4301 [RFC4301], and IKEv2 RFC 4306 [RFC4306] RFC 4877 [RFC4877] RFCs is highly recommended.

1.1. Mobile IPv6

Mobile IPv6 provides the ability for a node (called "Mobile Node", MN) to be reachable at a permanent IPv6 address (its "Home Address", HoA) while its point of attachment to the network is changing (the temporary IPv6 address is called the "Care-of Address", CoA). One of the routers serving the prefix of the HoA has a special role in the mobility (this router is called the "Home Agent", HA.) Basically, the MN registers its CoA to its HA, then the traffic directed to the HoA is tunneled to the MN at its CoA. The correspondents can always use the HoA to reach the MN.

1.2. Dynamic keying

Mobile IPv6 also makes mandatory the use of IPsec to protect the messages (Binding Update, Binding Acknowledgement -- BU / BA) involved during the MN's registration to its HA. Dynamic keying represents the situation where a Key Management Protocol (such as IKE or IKEv2) is used for negotiating the Security Association ("SA") pair that will protect the BU/BA exchange (and optionnally other messages). We can distinguish two steps in the KMP exchanges. First, the peers negociate a secured channel ("IKE_SA"), based on some trust mechanism (shared key, certificates, ...). Then, using this secured channel, the peers can negociate the SA parameters for protecting the BU/BA and optionnally other traffic. Since the BU/BA exchange has not yet been completed when the SA are negociated, the HoA cannot be used, and therefore the IKE_SA is negociated using the CoA on the MN side. The child SA (the IPsec SA that protects the

BU/BA) is established between the HoA and the HA.

1.3. Movement

When the MN changes its CoA, the IPsec rules are updated to reflect this change. For the transport-mode SA, there is no update needed since the SA are established between the HoA and the HA. The tunnel-mode SA and SP entries must be updated. The IKE_SA (used only to protect IKE messages) endpoints may or may not be updated. The "K flag" as discussed in this document is meant to represent the ability of the peer to update the IKE_SA endpoints.

1.4. Requirements Language

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 RFC 2119 [RFC2119].

2. Problem statement

It has already been proved that if both peers (MN and HA) behave in the same way with regards to updating their IKE_SA endpoints or not, then the sequence of signaling messages on movements results in smooth operation.

This document will consider the situation where the peers behave differently (one peer updates the IKE_SA endpoint, the other does not.) The purpose is to highlight the value of the information negociated through the (K) flag.

The initial state for both scenario is as follow:

MN is on a Foreign Link 1 (with CoA1) and registered to its HA. We have the following links:

* IKE_SA established between CoA1 and HA

* SA1 (transport) between HoA and HA.

* SA2 (tunnel) between CoA1 and HA.

Then MN moves to Foreign Link 2 with CoA2.

2.1. Scenario 1: HA updates its endpoints (K=1), MN does not (K=0).

Step 1: The BU message is sent using SA1.

* SA2 is updated on the MN to CoA2.

Step 2: The HA receives the BU.

* It updates its IKE_SA remote endpoint

* It updates its SA2 remote endpoint.

* It sends the BA using SA1.

Now, we have two possibilities concerning the next IKE message:

1. The MN needs to send an IKE message to the HA.
   In this case, since the IKE_SA source address is not valid anymore, we have to establish a new IKE_SA using the CoA2 address. This is the same behavior as case K=0 for both hosts. Instead of establishing a new IKE_SA, the MN may choose to use another available address as source address to send the IKE message. This must be done with care, since the HoA must not be used. In that case it is the same as case K=1 for both hosts.

2. The HA needs to send an IKE message to the MN.
   In this case, the MN receives the message. It may choose to update its IKE_SA local endpoint according to the dst address in the message, in which case the exchange will succeed. It may also choose to discard the message silently. In that case, the HA will end up in being unable to negociate the SA and therefore mark the IKE_SA (and all its CHILD_SA in IKEv2) as dead. Negotiation of a new IKE_SA will happen only when a new ACQUIRE message occurs.

Note that the second case is less likely to happen than the first, since the MN is always the initiator of first IKE exchanges and shorter lifetime values should be used for SA on the MN.

2.2. Scenario 2: MN updates its endpoints(K=1), HA does not (K=0).

Step 1: The BU message is sent using SA1.

* SA2 is updated on the MN to CoA2.

* IKE_SA is updated on the MN to CoA2.

Step 2: The HA receives the BU.

* SA2 is updated on the HA.

Then, again, we have two possibilities concerning the next IKE message:

1. If MN wants to send an IKE message to HA.
   HA receives a message from a new unknown address, with a valid SPI identifier. Implementation may choose to discard silently the message (to protect against DoS attacks for example). In this case, the MN receives no answer and invalidates the IKE_SA and the dependent SA. New negotiation will have to occur later, which is time-consuming. During this timeframe, upper-layer flow is interrupted. Implementation may also choose to accept the message from the unknown IP address. In that case, the reply will be sent to the new address, and it is equivalent as if the

HA had updated the IKE_SA endpoints.

2. If HA wants to send an IKE message to MN.
   It sends the message to the wrong address (CoA1). It results in the IKE_SA (and CHILD_SAs) being invalidated after the timeout (and retries, which may last for some minutes). This situation will prevent the HA from being able to forward packets to the MN and may be complicated to resolve (will need to wait for MN to detect dead peer and re-establish a new IKE_SA). This will result in an even bigger interruption in upper-layer flow.

3. Conclusion

Here is a summary of the several possibilities in dynamic keying

after a movement.

- If both MN and HA have the capability of updating the IKE session endpoints, then there is no need to re-create a session after movement and we have no additionnal interuption in the upper-layer flow, but the handover time.

- If both peers do not have this ability, then next time an IKE message needs to be exchanged, it will results in creating a new IKE session. In the usual case, we do not need to wait for an IKE timeout, since the MN can not use the old address anymore.

- If one peer updates the IKE session endpoint and the other does not, it results in a bad situation where we have to wait for IKE timeout (several minutes) before re-establishing a clean IKE session. Upper-layer traffic may be interrupted during this delay.

To ensure smooth operation, when the (K) flag negotiation after BU/BA exchange has shown that the remote peer does not support the IKE session movement, the local host MUST NOT update its IKE session endpoints after a movement.

We can shorten the delay by deleting the broken IKE_SA after the movement occurs (after BA has been emitted and received). An implementation SHOULD require this deletion when the remote peer does not support the IKE_SA movement. This would force next message to trigger an ACQUIRE and a new IKE session to be established.

Note that if the support for migrating the IKE session is mandatory, as is the support for migrating the tunnel-mode SA, then is simplifies the problem and removes the need for (K) flag.

4. IANA Considerations

This memo includes no request to IANA.

5. Security Considerations

This is not relevant for this draft.

6. References

6.1. Normative References

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

6.2. Informative References

[I-D.narten-iana-considerations-rfc2434bis]
Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", draft-narten-iana-considerations-rfc2434bis-08 (work in progress), October 2007.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

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

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

[RFC4306] Kaufman, C., "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.

Author's Address

Sebastien Decugis
University of Tokyo
Keio University Murai Lab., 144-8 Ogura, Saiwai-ku
Kawasaki, Kanagawa 212-0054
JP

Phone: +81 44 580 1600
Email: sdecugis@hongo.wide.ad.jp

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).