Internet Engineering Task Force
Internet Draft
Expires in July 2004

Wassim Haddad
Ericsson Research Canada
Helsinki University of Technology
Francis Dupont
ENST de Bretagne
Lila Madour
Suresh Krishnan
Ericsson Research Canada
Soohong Daniel Park
Samsung Electronics

February 2004

Optimizing Mobile IPv6 (OMIPv6)

<draft-haddad-mipv6-omipv6-01.txt>

Status of this memo

Abstract

Mobile IPv6 protocol introduced the route optimization mode to allow a direct exchange of data packets between the mobile node (MN) and the correspondent node (CN). This memo is a proposal to optimize the Mobile IPv6 solution, by reducing the handoff

latency and the number of signaling messages.

Table of contents

1. Introduction

Mobile IPv6 [1] introduced the route optimization (RO) mode to allow a direct exchange of data packets between a mobile node and a correspondent node (CN). Such mode is efficient, but it raises many security concerns and generates an excessive amount of redundant mobility signaling messages.

According to [1], these signaling messages are needed to periodically create a shared secret between the MN and the CN.

This memo describes an optimization to the RO mode, which aims to enhance its efficiency by making it less vulnerable, while keeping it at least as secure as it is in the RO mode and by reducing the high number of redundant signaling messages as well as the handover latency.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", "MAY" in this document are to be interpreted as described in RFC 2219 [2].

3. Terminology

DH Message

Diffie-Hellman message that is made by Diffie-Hellman algorithm.

RO

Route Optimization mode which allows the correspondent node to route data packets directly to the MN's care-of address. The RO mode requires the MN to register its new IP address with the Correspondent node.

Kabm

The shared secret resulting from a DH exchange. Kabm refers in this draft to the "Authenticated Binding Management" key that is used to authenticate the mobility signaling messages.

MiTM attack

Man-in-The-Middle attack, which is able to be launched through the spoofing of DH messages.

Note that most related terminologies used in this document are described in more details in [1].

4. Motivation

The RO mode allows the MN to talk directly to the CN, i.e, by using the direct path between them. In order to do so, the RO mode requires both entities to compute a shared secret (i.e., Kbm) in order to authenticate the binding updates (BUs) and binding acknowledgments (BA) messages with the same shared secret.

For security reasons, it is required that the lifetime of the shared secret be reduced to few minutes, thus obliging both entities to re-create a new Kbm at a high frequency. For more information about the security concerns and necessary defenses related to the RO mode, please refer to [4].

Each time the MN needs to compute a fresh Kbm, it needs to exchange four messages with the CN, i.e., to run the return

routability (RR) procedure. The loss of any of the four

messages requires the exchange of at least two additional messages with the CN. Note that for security reasons, the MN's home agent (HA) MUST get involved each time the RR test is performed.

If the RR test succeeds (i.e., the MN and the CN compute a Kbm shared secret), the MN must send a BU message to its HA and waits for a BA. Upon receiving a BA from its HA, the MN sends a BU to its CN to update its binding cache entry (BCE) with its new location (i.e., care-of address (CoA)) and waits for a BA.

The BUs authentication procedure requires approximately 1.5 round trips time between the mobile node and each correspondent node (for the entire RR procedure in a best case scenario, i.e, no packet loss) and one round trip time between the MN and the HA. Needless to mention that the delay resulting from such redundancy is NOT acceptable for time sensitive applications.

Note that each time the MN performs an RR test, 2 messages are exchanged in clear between the MN and the CN and two others are exchanged in clear between the HA and the CN across the Internet, thus exposing all the vulnerabilities and critical ingredients every few minutes during the ongoing session.

It becomes clear from the above that the RO mode introduces an expensive efficiency in terms of excessive mobility signaling messages, high latency and many security concerns.

This draft describes one way to make the exchange of BU/BA messages safer and substantially reduce the number of mobility signaling messages as well as the latency of the handover.

5. Overview of OMIPv6

The OMIPv6 proposal is a practical aspect of the trade-off suggested by S. Bradner, A. Mankin and J. Schiller in the Purpose-Built Keys (PBK) framework [3]:

"However, there are many circumstances where we can improve overall security by narrowing the window of vulnerability, so that if we assume that some operation is performed securely, we can secure all future transactions".

One of the main advantages for using OMIPv6 is that it gives a malicious node only ONE chance to launch a successful attack against the HoT and/or CoT messages, thus narrowing the window of vulnerability to the minimum.

This advantage becomes more critical when the random parameter

is added. Actually, switching to OMIPv6 can occur at anytime, any location and at any stage during the ongoing session.

At the opposite, if the assumption is wrong, all future transactions are compromised, i.e., attacks are made more difficult and very limited in time but when they succeed their effects last for a longer time.

Such assumption is reasonable with regards to security needs since it is based on the MIPv6 security design, and offers better performance for the rest of the ongoing session.

The suggested solution should be implemented on top of the current MIPv6 architecture. OMIPv6 utilizes the RR test procedure, which has been designed in [1] and SHOULD NOT be used alone.

OMIPv6 allows to compute a shared secret secret, which is longer than the one created in MIPv6, thus making it more difficult to crack.

OMIPv6 substantially reduces the amount of mobility signaling messages by eliminating the need for the CoTI/CoT and HoTI/HoT messages in normal situation. Such reduction will result in a reduced handover latency.

Another feature is that OMIPv6 does not require the deployment of an infrastructure to distribute keys, thus eliminating any scalability problems.

6. OMIPv6 Operation

OMIPv6 consists on deriving a long shared secret which will be used by both entities to authenticate the BU/BAs messages. The new shared secret is derived from a DH exchange, which SHOULD be launched by the MN immediately after a successful RR test. Further DH procedures MAY be performed later during the session and MUST NOT rely on an RR test.

After a successful RR test, the MN and the CN will share a secret (Kbm). This key MUST be used to authenticate the DH messages exchanged between the CN and the MN. Note that using the shared secret resulting from the RR test enables also both nodes to authenticate each other.

The DH messages MUST be exchanged on the same paths used to exchange the RR test messages. For this purpose, the MN MUST

sign the first DH message with the Kbm and send it to the CN

via the direct path. The MN MUST include its home address by using a home address option (HAO).

The CN's reply to the first message MUST also be signed with the Kbm, duplicated and both copies MUST be sent to the MN: One copy MUST be sent via the direct path and another copy via the path going through the MN's HA.
If the MN finds the two messages identical, then it pursues the DH exchange and sends the third message via the direct path.

The CN ends the procedure by sending the fourth DH message on the same path.

Note that the main objective behind duplicating the second DH message is the potential ability to reveal a possible MiTM attack on the first one (i.e., if the malicious node knows the Kbm). By duplicating the second DH message, a successful MiTM attack will consist on attacking two duplicated messages sent on two different paths at the same time, which will probably make such kind of attack more difficult.

The DH exchange will allow both entities to compute a long shared secret (Kabm), and to establish a bidirectional security association (SA) between them without the need to rely on any existing public key infrastructure.

The Kabm MUST be used to authenticate the Binding Update (BU), Binding Acknowledgement (BA) messages exchanged between the MN and the CN.

In order to reduce the handover latency, the MN will send the BU on the direct path immediately after receiving a BA message from its HA. Note that the MN MAY duplicate the BU message and send a copy on the path going via its HA. Only one copy is enough to update the CN's binding cache entry. In this case, the BU sent via the HA MUST have the same sequence number than the one sent via the direct path.

When the CN gets a valid BU signed with the Kabm, it will update its BCE, send a BA message to the MN and continue the session.

The CN will continue the session immediately after sending the BA.

After establishing a bidirectionnal SA between the MN and the CN, the following rules MUST be applied:

- The MN MUST NOT use the alternate care-of address option in

the BU message sent to the CN in order to counter a third

party bombing attack [6].

- The MN MUST NOT use the nonce indices option in new binding updates messages sent after a care-of address change.

The MN SHOULD set the Acknowledge (A) bit in the BU message after switching to OMIPv6.

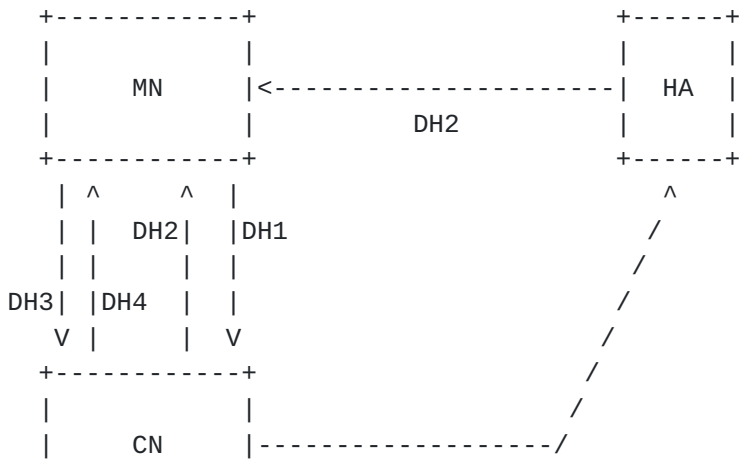
To avoid replay attacks, the MN will keep the sequence number sent in the first BU immediately after a DH exchange and increment it in all subsequent BU messages.

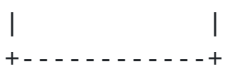
7. The Diffie-Hellman Exchange

The DH exchange can be launched at any time during the ongoing session. In order to reduce the amount of signaling messages to the minimum, it MAY be launched, for example, immediately after running the first RR test.

The update of the Kabm MAY be done periodically or each time after the MN switches to a new network. The DH procedure MAY be done in parallel with the ongoing session and the resulting new Kabm SHOULD be used to refresh the CN's BCE with the current MN's CoA.
After completing a DH procedure, any new mobility signaling message MUST be signed with the new Kabm computed from the DH exchange. The two endpoints SHOULD silently drop any mobility message related to the MN's IP home/care-of address or the CN's address and not signed with the Kabm.

The scheme below shows the different paths taken by the four messages of a DH exchange between a MN and the CN:




DH2

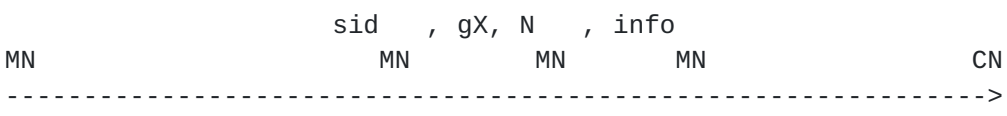
As it has been mentioned, the DH messages MUST be authenticated from both sides by using the Kbm. The contents and the signature associated with each DH message has been detailed in [5].

In OMIPv6, the DH messages exchanged between the two MNs are described in the following:

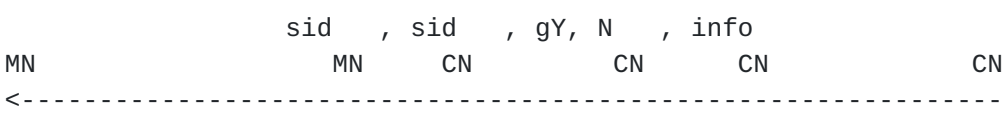
7.1 The DH messages structures:

The DH message structure is shown in the following:

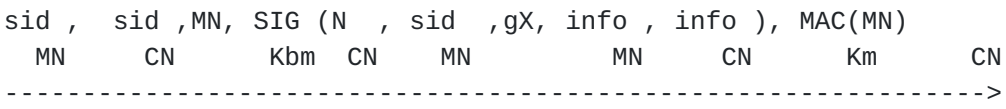
- DH1 message structure:



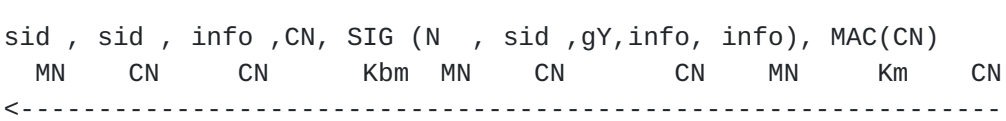
- DH2 message structure:



- DH3 message structure:



- DH4 message structure:



In the above scheme, the following abbreviations have been adopted:

- gX = shared part of MN's secret
- gY = shared part of CN's secret
- sid = session identifier used to specify the ongoing session.
- N = nonce
- info = additional information carried in the protocol messages
- MN = Identity of MN
- CN = Identity of CN
- Kbm = key generated from the RR test
- SIG(msg) = denotes the signature of "msg" using the Kbm.
- Km = key generated from DH (known only by the MN and the CN)
- MAC(msg) = denotes a message authenticated code computed
  Km from "msg" and signed by Km.

8. Security considerations

The design principle of base MIPv6 RO is the establishment of bindings using a security-wise "weak" authentication scheme, but at the same time limiting the set of possible attackers to a certain path and limiting the potential consequences of an attack to bindings of short duration.

This draft proposes an alternative mechanisms where different design tradeoffs have been incorporated. In particular, we increase the strength of the authentication mechanism while at the same time allowing a more permanent binding.

The DH mechanism is performed without authentication beyond the usage of the original Kbm provided from RR, which is used to authenticate the BU/BA messages in MIPv6.

9. Acknowledgements

Authors would like to thank Laurent Marchand and Jari Arkko for reviewing the draft. Authors gratefully thank Erik Nordmark for his valuable inputs on the concept.

10. Normative References

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

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

11. Informative References

[3] S. Bradner, A. Mankin and J. Schiller, " A Framework for Purpose-Built Keys (PBK)". draft-bradner-pbk-frame-06.txt, October 2003.

[4] P. Nikander, T. Aura, J. Arkko, G.Montenegro and E. Nordmark "Mobile IP version 6 Route Optimization Security Design Background", draft-nikander-mobileip-v6-ro-sec-01.

[5] Krawczyk, H., "SIGMA: the 'SIGn-and-MAC'Approach to Authenticated Diffie-Hellman and its use in the IKE Protocols", in Advanceds in Cryptography - CRYPTO 2003 Proceedings, LNCS 2729, Springer, 2003. Available at:

http://www.ee.technion.ac.il/~hugo/sigma.html.

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

12. Author's Addresses

Wassim Haddad
Ericsson Research Canada
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
CANADA
Phone: +1 514 345 7900
Fax: +1 514 345 6105
E-Mail: Wassim.Haddad@lmc.ericsson.se

Francis Dupont
ENST de Bretagne
Campus de Rennes
2, rue de la Chataigneraie
BP 78
35510 Cesson Sevigne Cedex
FRANCE
Fax: +33 2 99 12 70 30
E-Mail: Francis.Dupont@enst-bretagne.fr

Lila Madour
Ericsson Research Canada
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
CANADA
Phone: +1 514 345 7900
Fax: +1 514 345 6195
E-Mail: Lila.Madour@ericsson.com

Suresh Krishnan
Ericsson Research Canada
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
CANADA
Phone: +1 514 345 7900
Fax: +1 514 345 6195
E-Mail: Suresh.Krishnan@ericsson.com

Soohong Daniel Park
Samsung Electronics

Mobile Platform Laboratory, Samsung Electronics

416. Maetan-Dong, Yeongtong-Gu, Suwon
Korea
Phone: +81 31 200 4508
E-Mail: soohong.park@samsung.com

13. Full Copyright Statement