Internet Engineering Task Force
Mobility Privacy
Internet Draft
Expires December 2005

Wassim Haddad
Suresh Krishnan
Ericsson Research
Francis Dupont
Point6
Marcelo Bagnulo
UC3M
Hannes Tschofenig
Siemens
June 2005

Anonymity and Unlinkability Extension for CGA-OMIPv6

<draft-haddad-privacy-omipv6-anonymity-00>

Status of this Memo

Abstract

The "Optimized Mobile IPv6 with CGA" [CGA-OMIPv6] protocol specifies a new route optimization (RO) technique. This document

describes a new extension to be added to the CGA-OMIPv6 protocol in order to provide the anonymity and the unlinkability at the IP layer.

Table of contents

1. Introduction

CGA-OMIPv6 (called "OMIPv6" in the rest of the document for simplicity) protocol specifies a new route optimization (RO), which reduces the amount of signaling messages, the handover latency and improves the overall security.

However, OMIPv6 protocol lacks privacy support, namely anonymity/pseudonymity and unlinkability. Supporting these privacy aspects in OMIPv6 would allow a mobile user to move outside its home network without disclosing its real IPv6 home address, and thereby to prevent the ability to correlate actions at this layer.

This document describes privacy extensions to the OMIPv6 protocol.

2. Terminology

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

3. Glossary

Anonymity

Anonymity ensures that a user may use a resource or service without disclosing the user's identity.

Anonymity in wireless networks means that neither the mobile node nor its system software shall by default expose any information, that allows any conclusions on the owner or current use of the node.

Consequently, in scenarios where a device and/or network identifiers are used (e.g., MAC address, IP address), neither the communication partner nor any outside attacker should be able to disclose the relationship between the respective identifier and the user's identity.

Pseudonymity

Pseudonymity is a weaker property related to anonymity. It means that one cannot identify an entity, but it may be possible to prove that two pseudonymous acts were performed by the same entity.

Unlinkability

Two events are unlinkable if they are no more and no less related than they are related concerning the a-priori knowledge.

Unlinkability ensures that a user may make use of resources or services without others being able to link the use of these services together.

In hiding the mobile node's current location, unlinkability feature removes any possible correlation between two successive IP handovers performed by the same mobile node.

For more information about privacy aspects and location privacy please refer to [MOMIPRIV].

4. Problem Statement

OMIPv6 protocol introduces a new route optimization (RO) mode, which reduces the load of signaling messages, i.e., mainly by eliminating the HoTI/HoT messages, offers a semi-permanent security association (SA) between the mobile node (MN) and the correspondent node (CN) and improves the overall security of the MN <-> CN communication.

However, OMIPv6 allows the CN and any potential eavesdropper located on the path between the MN and the CN to first identify the mobile node via its IPv6 Home Address (HoA) and then to trace its movements in real time across the Internet, thus seriously violating its privacy. Such scenario is feasible by simply looking into the Binding Update (BU) message(s) sent by the MN to the CN, which carries among other parameters, the MN's HoA and its new current topological location, i.e., disclosed in its care-of address (CoA).

In addition to the BU message(s), the eavesdropper can learn and trace the MN's movements by looking into the data packets exchanged with the CN.
In fact, the main RO mode (detailed in [MIPv6]) defined two mobility extension headers, which carry the MN's home address. The first one is the Home Address Option (HAO) and is inserted in each data packet sent by the MN to the CN on the direct path. The second one is a Routing Header (RH) and is inserted in each data packet sent by the CN to the MN on the direct path.

Based on the above, it appears that in order to keep the exchange of data packets between the two endpoints flowing on the direct path, only the home address can be hidden from both the CN and any potential eavesdropper(s) located on the direct path.
Consequently, any solution for the privacy problem in OMIPv6 MUST prevent the CN from falling back to the bidirectional (BT) mode under any circumstance(s), since data packets sent by the CN are addressed to the MN's HoA. The BT mode is detailed in [MIPv6].

But it should be noted that replacing the real MN's HoA with a static (or even dynamic) pseudo-HoA can still allow the eavesdropper to correlate between MN's movements across the Internet, thus breaking the unlinkability feature. Such correlation can be accomplished by simply tracing the BU messages via the sequence number carried by each message. The seriousness of such correlation is tightly related to how

difficult is for the eavesdropper to discover the MN's real HoA
(e.g., based on prior knowledge and/or other identifier(s),
which are already known or can be discovered at a further stage,

etc). In fact, such knowledge can reveal all MN's pseudo-HAs and their corresponding CoAs as well as the exact time of each movement.

The unlinkability feature can also be broken if an eavesdropper is able to correlate between two data packets exchanged between the MN and the CN and carrying different CoAs, but associated to the same pseudo-HoA. Such correlation may reveal the exact time of the MN's movement(s) regardless of the content of the BU message. In addition, tracing the BU message may also help the eavesdropper correlate between the MIPv6 signaling messages and the data packets (namely the pseudo-HoA and/or CoA carried by the BU message with the address(es) carried by the data packet.

Consequently, we argue that any solution for privacy related to the network layer mobility only should also offer the unlinkability feature by fulfilling the following requirements:

- prevent disclosing the MN's HoA in any BU message.
- avoid using the same pseudo-HoA in more than one BU message.
- prevent the possibility of tracing the BU messages via the sequence number.
- prevent any correlation between data packets exchanged with the current CoA and the next BU message sent after performing an IP handover.
- prevent any correlation between data carried by the BU message and data packets exchanged after receiving the BA message.

Finally, it should be noted that any potential solution, which addresses privacy as motivated above, should take the scenario where a mobile node starts communicating end-to-end with a CN from its home network before switching to a foreign network(s) into consideration.

5. Proposed Solution

Our suggested solution can be used regardless of whether the MN is establishing its session from its home network or from a visited network. It consists of three components:

a) the "P" bit that is carried in the Pre-Binding Update (PBU), the Pre-Binding Test (PBT) and the Binding Update (BU) message; this bit demands additional processing guidelines (including sequence number handling).

b) replacing the home address carried within the Home Address Option (HAO) with an ephemeral identifier.

c) associating the interface identifier (iid) of the MN's home address with the cryptographically-Based Identifiers (CBID).

As a first step, a Pre-Binding Update (PBU) message is sent directly from the MN to the CN. The PBU message carried a newly introduced Privacy (P) bit set and thereby asks the CN to skip any home address test, and also to avoid any possible fallback to the bidirectional tunneling mode (described in [MIPv6]) during the subsequent data exchange.

The MN MUST set the "P" bit in the PBU message, regardless of the MN's location (also while staying at the home network), and in the BU message sent after receiving the Pre-Binding Test (PBT) message from the CN.

Additionally, the MN MUST replace the home address inserted in the Home Address Option (HAO) with a "Virtual Home Address" (VHoA). The VHoA sent in the first BU message MUST be a statistically unique cryptographically generated and verifiable identifier [CBID]. Note that using the CBID technology in Mobile IPv6 for privacy purposes has been introduced in [MIPriv].

During the first exchange of signaling messages between the two endpoints, and in order to enable the CN to check if it is still talking to the same MN when receiving the first BU message, the MN MUST insert in the PBU message the value obtained from hashing the VHoA (note that in this case, the VHoA is the CBID, thus the value is equal to SHA1(CBID) in the PBU message.

After receiving the PBU message, the CN computes a challenge from the MN's CoA, the content of the HAO and a local secret. Then it inserts the challenge into the PBT message and returns it to the MN. When the MN gets the PBT message, it sends a BU

message carrying the "P" bit, the challenge and inserts the real CBID into the HAO. Note that the iid of the MN's CoA sent in the

PBU and the BU messages SHOULD be generated from hashing the CBID in the following way:

iid(CoA) = First(64, SHA1(CBID))

Where:

- SHA1 is a hashing function
- CBID is a cryptographically generated identifier
- First(size,input) is a function used to indicate truncation of the input data so that only the first size bits remain to be used.
- iid is the interface identifier

Upon receiving the first BU message with the "P" bit set, the CN starts by checking its validity. For this purpose, it will hash the content of the HAO, i.e., the CBID, and compares the first 64 bits of the resulting hash with the CoA's iid. After that, it will re-compute the challenge and compare it to the one sent in the message. The third step after a successful validation would be to create an entry in the BCE for the MN's VHoA and the CoA. The CN computes also a long lifetime shared secret (i.e., SKbm) and sends it back to the MN in the BA message as described in [OMIPv6].

The presence of the "P" bit in the BU message is also used to request the CN to replace the sequence number carried by the BU message, in its BCE with the "next" value, i.e., expected in the next BU message sent by the MN. Such value is called the "Sequence Value" SQV and is used to prevent replay attacks and to allow the CN to identify the MN's corresponding entry in its BCEs when processing a BU message carrying the "P" bit.

In OMIPv6, each time the MN sends a BU message, it MUST increment the sequence number. With the privacy extensions introduced by this document, both endpoints MUST increment the SQV with a constant value equal to the one obtained from hashing the SKbm. Finally, the incremented SQV is hashed, inserted by the MN into the BU message and sent it to the CN.

The two entities MUST compute the next SQV (nSQV) in the following way:

Khbm = SHA1(SKbm)

nSQV = First(64, SHA1((pSQV) | Khbm))

Where:

- SKbm is a long lifetime binding management key
- Khbm is the hashed binding management key
- pSQV is the previous SQV, i.e., SQV sent in the last BU message sent by the MN and already processed by the CN.
- nSQV is the hasht value of the next SQV computed during updating the BCE with the BU message carrying the pSQV.

The CN MUST compute and store the nSQV during creating/updating the MN's entry in its BCE, and the MN MUST compute and send a new SQV in all subsequent BU messages sent to the CN.

In addition, all subsequent BU messages sent after the first one, SHOULD carry a VHoA, which is generated from hashing the nCoA, i.e., nVHoA is equal to SHA1(nCoA), sent in the message.

However, it should be noted that the CN SHOULD NOT store in the MN's corresponding entry the new CoA (nCoA) and new VHoA (nVHoA) carried in the BU message. In fact, besides computing the nSQV and storing it in the corresponding entry, the CN SHOULD also compute another address pair (CoA, VHoA) to be used in the data packets exchange following the BCE creation/update. These two addresses are called "expected CoA" (eCoA) and "expected VHoA" (eVHoA).

The two expected addresses are computed in the following way:

```
iid(eCoA) = First(64, SHA1(Khbm | nCoA Subnet Prefix))

eVHoA = SHA1(eCoA)
```

Where:

- nCoA is the MN's care-of address sent in the BU message.
- eVHoA is the pseudo-home address carried in the HAO and RH headers in all data packets.

The subnet prefix of the nCoA MUST be the same as the one sent by the MN in the BU message (note that this technique is similar to the one defined in [HBA]). Note that in such scenario, the CN MUST update the MN's entry in its BCE with the eCoA and eVHoA. However, the BA message sent to the MN MUST carry the nCoA and nVHoA.

As mentioned above, when the MN sends a BU message carrying the "P" bit, the SQV MUST be used alone by the CN to detect the presence of an entry corresponding to the MN in its BCE. If an entry containing the same SQV is found, then the CN SHOULD

proceed to check the signature before updating the corresponding entry with the eCoA, eVHoA and nSQV.

6. Packet Format

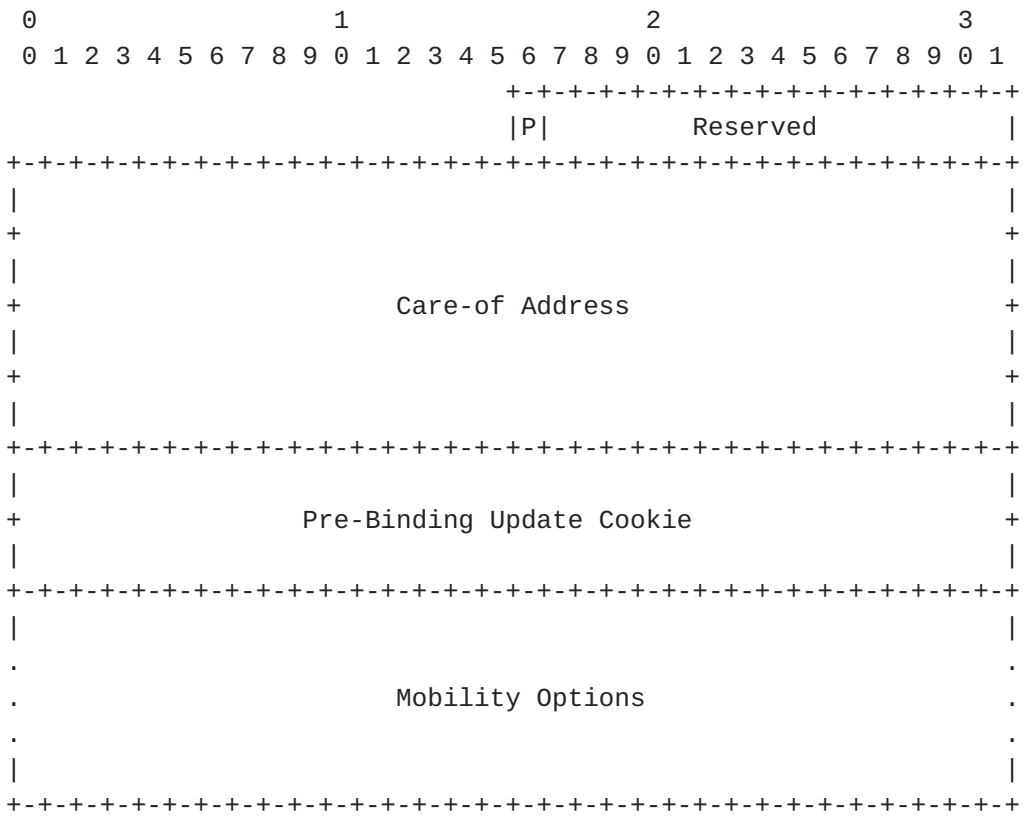
This proposal defines a new bit called the Privacy (P) bit to be added to the Pre-BU and BU messages. The MN MUST set the "P" bit in both messages and in all subsequent BU messages as long as it needs to keep its real home IP address undisclosed.

When used in the Pre-BU message, the "P" bit indicates to the CN to limit the address test to the CoA only and also to include the VHoA in computing the nonce value sent in the Pre-Binding Test (PBT) message.

When used in the BU message, the "P" bit is used for three different purposes. The first one is to ask the CN to use the sequence number to locate the MN's corresponding BCE. The second one is to notify the CN to NOT send any data packet carrying the MN's home pseudo-address, i.e., VHAO, as destination address.

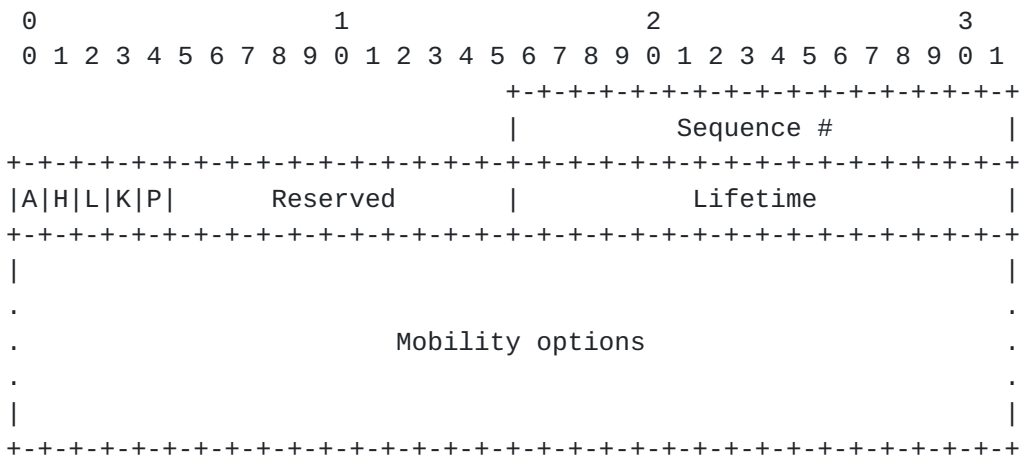
The third purpose is to ask the CN to compute the eCoA, the eVHoA, the new SQV and store them in the MN's corresponding BCE.

When used in the Pre-BU message, the structure of the message will be as it follows:



The different fields carried in the Pre-BU message are detailed in [OMIPv6].

When used in the BU message, the structure of the message will be as it follows:



The different fields carried in the BU message are detailed in [MIPv6].

7. Privacy Considerations

This memo describes an extension, which makes the MN's real identity anonymous for both the CN and any malicious eavesdropper(s) located on the path between the MN and the CN.

Our solution aims to present the MN's HoA as any other CoA that the MN may use during its movements across the Internet. However, our solution is based on the assumption that the BU messages exchanged between the MN and its HA are protected with an ESP tunnel according to [MIP6-IKE] and [MIP6-IKEv2].

The suggested solution provides the anonymity feature to the MN during exchanging data packets and signaling messages with the CN. It also provides the unlinkability feature during and after performing IP handovers, by making it difficult for an eavesdropper to correlate between two successive IP handoffs performed by the same MN. The unlinkability between these events aims to enhance the anonymity feature.
However, it should be noted that the unlinkability protection is limited against eavesdroppers located on the path between the MN and the CN and does not prevent the CN to trace the MN's movements in real time.

The suggested solution allows the MN to select when and where the anonymity feature should be activated. But it should be noted that it works only when the MN initiates the session. Actually, when the CN initiates the session, it uses the MN's home address (HoA). In such scenario, the MN can hide its current location from the CN by switching to the bidirectional tunneling mode.

It is worth mentioning that the anonymity concept is very much context dependent. In order to quantify anonymity with concrete situations, one would have to describe the system context, which is practically not always possible for large open systems [ANON].
Consequently, the efficiency of the suggested solution is strongly related to two key factors: the diversity and load of the traffic circulating in parallel with the MN's traffic, on the same portion(s) of the direct path, which is monitored by an eavesdropper(s).

Finally, the suggested solution strongly recommends using the Privacy Extension proposal [PRIVACY], in configuring the care-of address(es) sent by the MN in all BU messages except for the BU message sent after receiving a PBT message, i.e., in which the

CoA is derived from the CBID.

8. Security Considerations

The suggested solution does not introduce new attacks nor does it amplify threats. However, it is important to mention that it makes the switch to the MIPv6 BT mode impossible.

The suggested solution aims to hide the mobile user's real identity when moving outside its home network or from its home network to foreign networks. Making the MN anonymous (with regard to the used home address) to potential eavesdroppers may help to prevent attacks, thus improves the overall security.

9. Normative References

[CGA-OMIPv6] W. Haddad, L. Madour, J. Arkko and F. Dupont, "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)", draft-haddad-mip6-cga-omipv6-04, May, 2005.

[MIPv6] D. Johnson, C. Perkins and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[MIP6-IKE] J. Arkko, V. Devarapalli, F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[MIP6-IKEv2] V. Devarapalli, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", draft-ietf-mip6-ikev2-ipsec-01, February 2005.

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

10. Informative References

[ANON] A. Pfitzmann et al. "Anonymity, Unobservability, Pseudonymity, and Identity Management - A Proposal for Terminology", Draft v0.21, September, 2004.

[CBID] G. Montenegro, C. Castelluccia, "Cryptographically-Based Identifiers (CBID): Concepts and Applications", ACM Transaction on Information and System Security (TISSEC), February 2004.

[HBA] M. Bagnulo, "Hash Based Addresses (HBA)", draft-ietf-multi6-hba-00, December 2004.

[MIPriv] C. Castelluccia, F. Dupont, G. Montenegro, "A Simple Privacy Extension to Mobile IPv6", IEEE/IFIP International Conference on Mobile and Wireless

Communication Networks (MWCN), Paris, France, October

2004.

[MOMIPRIV] W. Haddad, E. Nordmark, F. Dupont, M. Bagnulo, S. Park and B. Patil, "Privacy for Mobile and Multi-homed Nodes: MoMiPriv Problem Statement", draft-haddad-momipriv-problem-statement-01, February 2005.

[PRIVACY] T. Narten, R. Draves and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", draft-ietf-ipv6-privacy-address-v2-04, May 2005.

11. Authors' Addresses

Wassim Haddad
Ericsson Research
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
Canada

Phone: +1 514 345 7900 (#2334)
E-Mail: Wassim.Haddad@ericsson.com

Suresh Krishnan
Ericsson Research
8400, Decarie Blvd
Town of Mount Royal
Quebec H4P 2N2
Canada

Phone: +1 514 345 7900 (#2871)
E-Mail: Suresh.Krishnan@ericsson.com

Francis Dupont
Point6
c/o GET/ENST Bretagne
Campus de Rennes
2, rue de la Chataigneraie
CS 17607

35576 Cesson-Sevigne Cedex
France

E-Mail: Francis.Dupont@enst-bretagne.fr

Marcelo Bagnulo
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: +34 91 6249500
E-Mail: marcelo@it.uc3m.es
URI: http://www.it.uc3m.es

Hannes Tschofenig
Siemens AG
Otto-Hahn-Ring 6
81739 Munich
Germany

EMail: Hannes.Tschofenig@siemens.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement