Network Working Group
Internet-Draft
Expires: August 21, 2006

F. Dupont
CELAR
W. Haddad
Ericsson Research

February 17, 2006

Optimizing Mobile IPv6 (OMIPv6)
draft-dupont-mipshop-omipv6-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes an optimization to the Mobile IPv6 (MIPv6) protocol, which uses the crypto-based identifier (CBID) technology to securely establish a long lifetime bidirectional security association (SA) between the mobile node (MN) and the correspondent node (CN) and to reduce the IP handoff latency as well as the amount of signaling messages.

Table of Contents

1. Introduction

Mobile IPv6 protocol as described in [MIPv6] introduces a new mode called route optimization (RO), which enables direct communication between the MN and the CN.

However, the RO mode requires a considerable amount of redundant signaling messages, which in turn create a significant latency problem and raises many security concerns. These problems are seriously undermining the possibility of any wide deployment of the RO mode in its current design.

This document describes an optimization to the Mobile IPv6 (MIPv6) protocol, which uses the crypto-based identifier [CBID] technology to securely establish a long lifetime bidirectional SA between the MN and the CN and to reduce the IP handoff latency as well as the amount of signaling messages.

2. Conventions used in this document

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 [TERM].

3. Problem Statement

MIPv6 RO mode security is based on the return routability (RR) procedure. The RR allows the CN to check the reachability of the MN's home address (HoA) and its new care-of address (CoA), and to enable both endpoints to share a secret, (Kbm), in order to authenticate the binding update and acknowledgment (BU/BA) messages exchanged between them.

The RR consists on exchanging four signaling messages, i.e., the HoTI/HoT and CoTI/CoT, between the MN and the CN, prior to sending a BU message to the CN. However, the CoTI/CoT messages are exchanged in clear on the direct path between the MN and the CN, and the HoTI/HoT messages are exchanged in clear between the MN's home agent (HA) and the CN. Consequently, such exchange raises many security concerns as it is open to many attacks.

In addition, it is required according to [MIPv6-Sec] to repeat the RR procedure during each IP handoff and/or during a maximum of 420 seconds, even if the MN does not move. Such requirement boost significantly the amount of signaling messages as well as the handoff latency and makes the HA a single point of failure.

In order to address the RR issues, a new proposal based on using the cryptographically generated address [CGA] is under design. The new proposal, i.e., [OMIPv6-CGA], allows the MN to provide the CN with a proof of ownership of its HoA's Interface Identifier (IID) and enables both endpoints to share a long lifetime shared secret. However, the suggested proposal does not allow the MN to provide any proof of ownership of its CoA's IID and is open to session hijacking and DoS attacks at some critical stage. It should be noted that these attacks don't require the malicious node to be located simultaneously on the HA-CN path and on the direct path between the two endpoints. In fact, launching these attacks require the malicious node to be located only on the path between the MN's HA and the CN (i.e., HA-CN).

OMIPv6-CGA requires the MN to perform one RR procedure (as defined in MIPv6) prior to establishing a long lifetime bidirectional security association (SA). For this purpose, when the MN moves for the first time to a foreign network or decide to switch to the RO mode from a foreign network, it MUST send a HoTI and CoTI messages to the CN. However, the fact that the (HoTI, HoT) pair of messages goes in clear between the HA-CN makes them visible to a malicious node located on the same path. Consequently, the malicious node can easily discover the home keygen token sent by the CN to the MN in the HoT message. In order to launch a successful attack against a MN using the OMIPv6-CGA procedure, the malicious node has to send the first BU message to the CN on behalf of the MN, i.e., before the MN sends its own BU message. For this purpose, the malicious node has to always keep at hand a fresh care-of keygen token. This can be easily done by using, for example its own IPv6 address to exchange at anytime a CoTI/CoT messages with the CN, in order to get a new care-of keygen token.

Sending a first and valid BU message to the CN, on behalf of the MN, allows the malicious node to hijack the MN's ongoing session and prevents it from establishing a long lifetime bidirectional SA with the CN. OMIPv6-CGA protocol requires that the first BU message received by the CN from the MN be authenticated with the Kbm and signed with the MN's CGA public key.

In this memo, we introduce an alternative solution to the CGA technology, which offers the same features described in [OMIPv6-CGA] and also prevents the attack described above.

4. Quick Overview of Crypto-based Identifiers (CBID)

A CBID is a 128-bit opaque identifier, which has a strong cryptographic binding with its components, i.e., generated from the MN's key pair. Consequently, using identifiers that satisfy the CBID

structure offers the advantage that other nodes, e.g., CNs, can safely trust the node when it claims ownership of that identifier.

A CBID is generated as follows:

CBID = First(128,SHA1 (imprint | PK))

where:
imprint is a 128-bit field, which is a random value.
PK is the MN's public key formatted as a DER encoding of the SubjectPublicKeyInfo structure.
SHA1 is a one way hash function.
| denotes a concatenation.
First(x,y) means that only the high order x bits are considered from the resulting hash value.

This memo introduces some changes to the procedure used to generate a CBID, in order to further reduce the possibility of having a collision. The new suggested method to generate a CBID consists of the three following steps:
1. Input = 128-bit imprint | Public Key
2. Hash = SHA256 (Input)
3. CBID = Encode_128 (Hash)
where Encode_128 is an extraction function, which output is obtained by extracting the first most significant 128-bit from the resulting hash, i.e., Encode_128 (Hash) = First (128, Hash).

5. Protocol Description

The following diagram shows the mobility signaling exchange between the MN and the CN for the initial contact:

1. MN to CN (via HA): Pre-Binding Update (PBU)
2a. CN to MN (via HA): Pre-Binding Acknowledgment (PBA)
2b. CN to MN (directly): Pre-Binding Test (PBT)
3. MN to CN (directly): Binding Update (BU)
4. CN to MN (directly): Binding Acknowledgment (BA)

The suggested protocol is described in the following steps:
- When the MN moves for the first time to a foreign network, it sends a Pre-Binding Update (PBU) message to the CN via its HA, i.e., the PBU message is encrypted between the MN and the HA. The PBU message contains the MN's HoA and CoA. In addition, the 64-bit HoA and CoA's IIDs MUST be configured from equally splitting the 128-bit crypto-based identifier. For example, the HoA's IID SHOULD be equal to the 64 rightmost significant bits and the CoA's IID should be equal to the remaining 64 bits.

- After receiving a PBU message, the CN computes two keygen tokens and sends them in two different messages, i.e., the Pre-Binding Acknowledgment (PBA) is sent via the MN's HA and MUST carry the home keygen token, and the Pre-Binding Test (PBT) is sent on the direct path and MUST carry the care-of keygen token.
  In order to prevent a malicious node located on the path between the MN's HA and the CN from hijacking the MN's ongoing session, by exploiting the discovery of the home keygen token sent in clear in the HoT message (as described earlier), this memo suggests that the CN MUST compute the two keygen tokens by using the MN's CoA and the 128-bit CBID. For this purpose, the home keygen token MUST be computed in the following way:
  ```
  Home Keygen Token :=
  First (64, HMAC_SHA1 (Kcn, (CBID | nonce | 0)))
  ```
  and the care-of Keygen token MUST be computed in the following way:
  ```
  Care-of Keygen Token:=
  First (64, HMAC_SHA1 (Kcn, (CoA | nonce | 1)))
  ```
  where HMAC_SHA1 is detailed in [HMAC], and Kcn and nonce are detailed in [MIPv6].
- When the MN gets the PBA and PBT messages, it combines the two tokens in the same way as described in [MIPv6], and uses the result to authenticate the BU message, which is sent on the direct path to the CN. In addition, the BU message MUST be signed with the MN's private key and MUST carry the 128-bit imprint and the MN's corresponding public key. For this purpose, this document defines a new option in the BU message to carry the imprint and use the same option defined in [OMIPv6-CGA] to carry the public key in the BU message.
- When the CN gets the BU message, it starts by checking the validity of the CBID. This is done by repeating the three steps described above, and comparing the resulting value with the one obtained from combining the two IIDs used in configuring the HoA and CoA. If the two values are identical, then the CN re-computes the two tokens and checks the authenticity of the the BU message. After that, the CN checks the RSA signature.
  If the signature is valid, then the CN creates a Binding Cache Entry (BCE) for the MN, computes a shared secret (SK) and encrypts it with the MN's public key. The CN inserts the encrypted SK in the BA message and sends it to the MN. The BA message MUST be authenticated with the shared secret.
- After checking the authenticity of the BA message, the MN decrypts SK with its private key and establishes the bidirectional SA. Note that the SA lifetime is by default 24 hours, after which the two nodes should re-key by repeating steps described above.
- After establishing the SA, all subsequent BU/BA exchange MUST be authenticated only with SK until the expiration of the SA. The RR procedure SHOULD NOT be repeated before the SK lifetime expires.

- For any subsequent IP handoff, the MN MAY autoconfigure its CoA by using as IID the first 64 bits resulting from hashing SK, the new network prefix and the previous CoA (pCoA), i.e.,
  CoA's IID:= First (64, SHA1 (SK | new network prefix | pCoA))

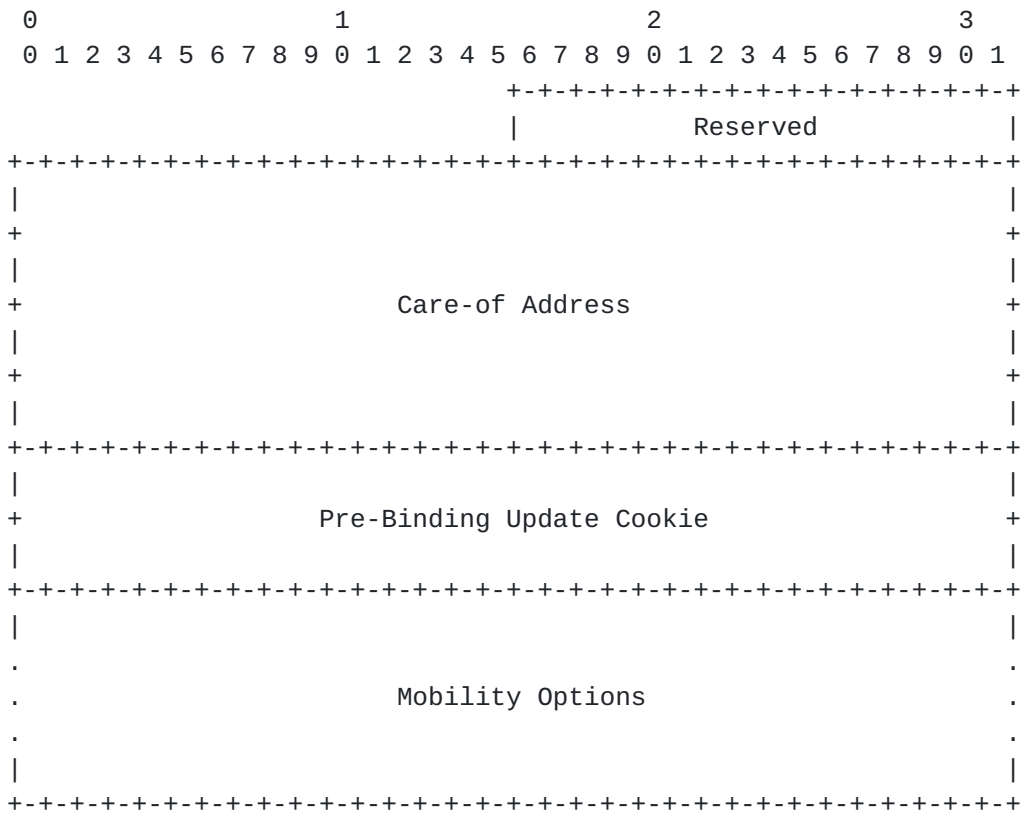
6. New Messages and Option Formats

Our proposal introduces 3 new messages and one new option, which are described in the following:

6.1. The Pre-Binding Update Message

This message is similar to a Binding Update message, but does not yet establish any state at the correspondent node. The purpose of this operation is to initiate the sending of two address reachability tests.

This message uses MH Type <To Be Assigned By IANA>. The format of the message is the following:



Reserved 16-bit field reserved for future use. This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Care-of Address
The current care-of address of the mobile node.

Pre-Binding Update Cookie
64-bit field which contains a random value, a cookie used to ensure that the responses match to requests.

Mobility Options
Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for this message.

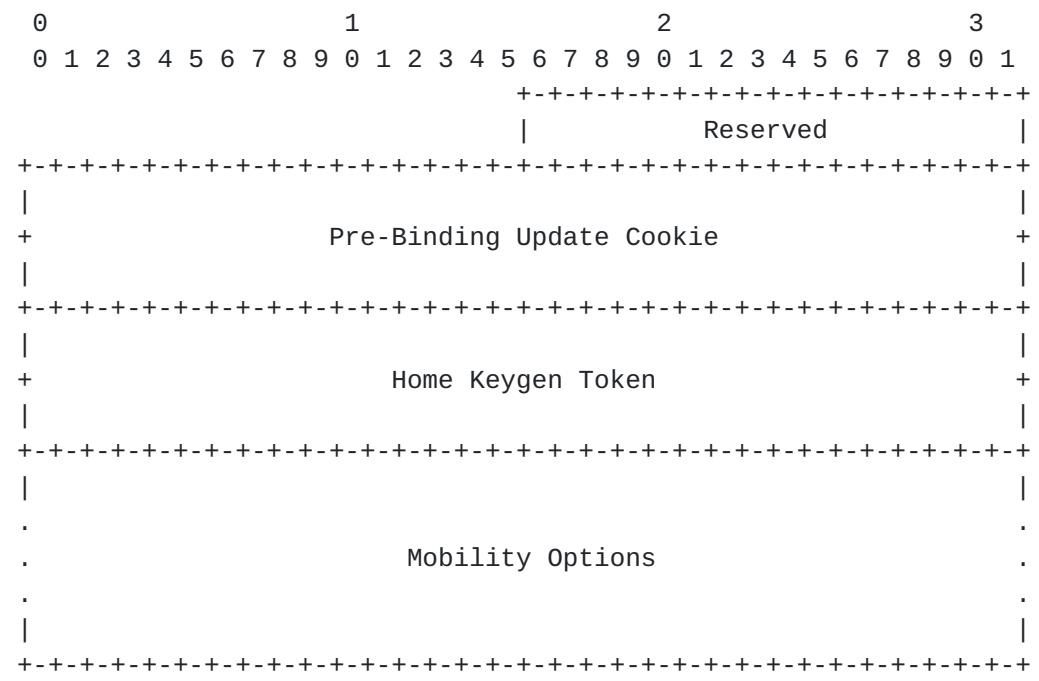
If no actual options are present in this message, no padding is necessary and the Header Length field will be set to 3.

This message is tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This protection is indicated by the IPsec security policy database, similarly to the protection provided for Home Test Init messages.

6.2. The Pre-Binding Acknowledgment (PBA) Message

This message acknowledges a Pre-Binding Update message. The purpose of this acknowledgment is to provide a part of the key Kbm required in the initial phase of our mechanism.

This message uses MH Type <To Be Assigned By IANA>. The format of the message is the following:



Reserved
16-bit field reserved for future use. This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Pre-Binding Update Cookie
This 64-bit field contains the value from the same field in the Pre-Binding Update message.

Home Keygen Token
This 64-bit field contains a Home Keygen Token, calculated as specified in RFC3775.

Mobility Options
Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for this message.

If no actual options are present in this message, no padding is necessary and the Header Length field will be set to 2.

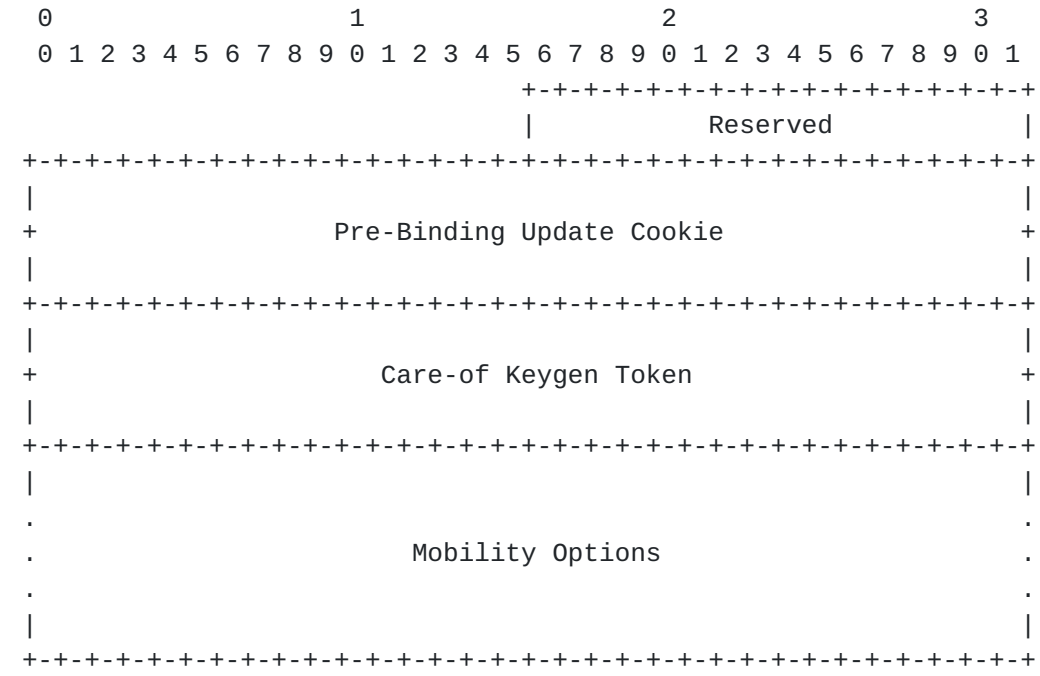
This message is tunneled through the home agent when the mobile node is away from home. Such tunneling SHOULD employ IPsec ESP in tunnel mode between the home agent and the mobile node. This

protection is indicated by the IPsec security policy database, similarly to the protection provided for Home Test messages.

6.3. The Pre-Binding Test (PBT) Message

This message also acknowledges a Pre Binding Update message, and ensures that the mobile node is reachable at its claimed address. The purpose of this acknowledgment is to provide the second part of the key Kbm required in the initial phase of our mechanism.

This message uses MH Type <To Be Assigned By IANA>. The format of the message is the following:



Reserved
16-bit filed reserved for future use. This value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Pre-Binding Update Cookie
This 64-bit field contains the value from the same field in the Pre-Binding Update message.

Care-of Keygen Token
This 64-bit field contains a Care-of Keygen Token, calculated as specified in RFC3775.

Mobility Options
Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. The receiver MUST ignore and skip any options which it does not understand. This specification does not define any options valid for this message.

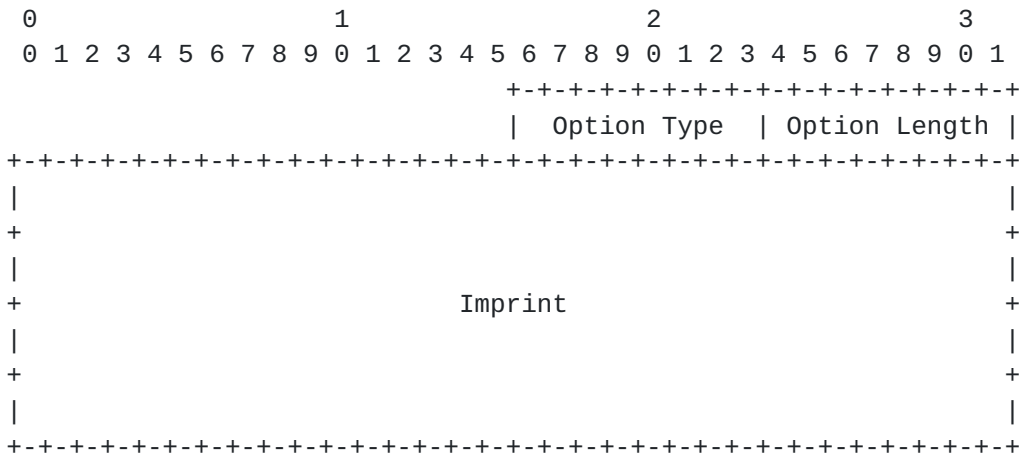
If no actual options are present in this message, no padding is necessary and the Header Length field will be set to 2.

6.4. The Imprint Option

This option is carried by the first BU message sent by the MN to the CN. The Imprint option allows the CN to check the ownership of the two IPv6 addresses, i.e., HoA and CoA, used in the BU message.

This option is used in the BU message structure described in [OMIPv6-CGA].

The option format is as follows:



Option Type
<To Be Assigned By IANA>.

Option Length
Length of the option = 16

Option Data
This field contains the 128-bit imprint value used to compute the CBID.

7. Security Considerations

This memo describes a solution, which addresses a particular security threat related to the presence of a static malicious node on the path between the HA and the CN. As described earlier, such threat can easily prevent the mobile node from establishing a long lifetime shared secret with the CN, and severely disrupts the other alternatives, which are limited to using the classic RO mode as defined in [MIPv6]. For this purpose, the suggested solution allows the MN to provide the CN with a double proof of ownership of its HoA and CoA IIDs and introduces a new way to compute the first home keygen token. Note that this document considers only the case of establishing a long lifetime security association.

The suggested solution offers a simple protection against this particular threat, and hence increases the overall security of the return routability procedure.

Finally, the suggested solution does not introduce nor enhance any new or existing threats to the return routability.

8. References

8.1. Normative References

[CGA] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3792, March 2005.

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

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

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

8.2. Informative References

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

[MIPv6-Sec] Nikander, P., Arkko, J., Aura, T., and E. Nordmark, "Mobile IPv6 version 6 Route Optimization Security Design Background", Internet Draft, draft-ietf-mip6-ro-sec-03.txt, June 2005.

[OMIPv6-CGA] Arkko, J., Vogt, C., and W. Haddad, "Applying Cryptographically Generated Addresses and Credit-Based Authorization to Optimize Mobile (OMIPv6)", Internet Draft, draft-arkko-mipshop-cga-cba-02.txt, October 2005.

Authors' Addresses

Francis Dupont
CELAR

Email: Francis.Dupont@point6.net

Wassim Haddad
Ericsson Research
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 #2334
Email: Wassim.Haddad@ericsson.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.