Network Working Group
Internet-Draft
Expires: January 12, 2006

H. Tschofenig
Siemens
W. Haddad
Ericsson Research

July 11, 2005

OMIPv6 Multi-Homing and Privacy
draft-tschofenig-omipv6-multihoming-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 12, 2006.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

The Optimized Mobile IPv6 with CGA (OMIPv6-CGA) protocol specifies a new route optimization (RO) to solve the mobility problem. Privacy extensions for OMIPv6 adds anonymity and unlinkability support to the OMIPv6-CGA protocol.

This document combines OMIPv6-CGA including its privacy extension with support for multi-homing. As such, it offers an efficient and

secure multi-homing and mobility support for MIPv6 using CGAs including privacy support.

Table of Contents

1. Introduction

Optimized Mobile IPv6 with CGA [I-D.haddad-mip6-cga-omipv6] protocol specifies a new route optimization (RO) to solve the mobility problem. Privacy extensions for OMIPv6 added anonymity and unlinkability support to the OMIPv6-CGA protocol.

This document combines these previously mentioned documents and adds multi-homing support. As such, it offers an efficient and secure multi-homing and mobility support for MIPv6 using CGAs with privacy support.

To provide multi-homing support based on [I-D.haddad-privacy-omipv6-anonymity] requires to deal with the following aspects:

- Ability to inform the other peer about the peer address set
- Ability to inform the other peer about the preferred address
- Ability to test connectivity along a path and thereby to detect an outage situation
- Ability to change the preferred address
- Ability to change the peer address set

Additionally, it is worth pointing out that a new care-of address must be authorized prior to its usage. The procedure detailed in OMIPv6 [I-D.haddad-mip6-cga-omipv6] and not repeated in this document. Finally, the aspect of state indexing needs to be considered. OMIPv6 selects the Binding Cache Entry (BCE) based on the Home Address. The privacy extensions defined for OMIPv6 modify this state selection approach and use a specially generated "Sequence Value" (SQV). Since this document builds on top of the privacy extensions for OMIPv6 SQV state indexing approach is reused.

2. Terminology

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 [RFC2119].

Terms, such as peer, peer address set, path or preferred address, are reused from MOBIKE [I-D.ietf-mobike-design]. Terminology related to OMIPv6 [I-D.haddad-mip6-cga-omipv6] and its privacy extension [I-D.haddad-privacy-omipv6-anonymity] can be found in the respective documents.

3. Strawman Protocol Proposal

This document requires the following protocol processing:

Ability to inform the other peer about the peer address set:

The MN indicates support for multihoming in the Binding Update with a new payload ADDRESS_LIST that is an extended version of the 'Alternate Care-of address' payload. This new payload also indicates the available addresses.

Ability to inform the other peer about the preferred address:

The source and the destination address of a packet directly sent to the CN is the preferred address pair.

Ability to test connectivity:

Procedures for path testing need further study. This procedure ensures that a currently used path stopped working. [Editor's Note: Some words about congestion control for concurrent path tests are needed.]

Ability to change the preferred address:

The source and the destination address of a packet directly sent to the CN is the preferred address pair. As a policy the MN thereby decides about the preferred address pair being used. This allows the protocol to work if stateful packet filtering firewalls are deployed in IPv6 networks.

Ability to change the peer address set:

The mobile node can change its peer address set at any time by sending a new Binding Update with a modified list of addresses in the ADDRESS_LIST payload.

[Editor's Note: Detailed protocol processing rules for the MN and the CN will be described in a future version of the document.]

4. Packet Format

Editor's Note: A future version of this document will define the following packet formats:
- Ability to carry the peer address set
- Ability to indicate the preferred address
- Ability to add / delete addresses from the peer address set.

5. Example

[Editor's Note: An example will be provided in a future draft version.]

6. Security Considerations

The security properties of the extension defined in this document are based on the OMIPv6-CGA [I-D.haddad-mip6-cga-omipv6] and subsequently on the security of CGAs (see [I-D.ietf-send-cga]). Privacy related aspects are discussed in [I-D.haddad-momipriv-problem-statement] and in [I-D.haddad-privacy-omipv6-anonymity] and applicable to this document. Mobility specific threats, such as traffic redirectly and hijacking, third-party flooding and blackholing, are addressed by the base OMIPv6-CGA proposal.

7. IANA Considerations

This document does not require actions by IANA.

8. Acknowledgments

The authors would like to thank Pasi Eronen for his work on the MOBIKE protocol [I-D.ietf-mobike-protocol].

9. References

9.1 Normative References

[I-D.haddad-mip6-cga-omipv6]
Haddad, W., "Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)", draft-haddad-mip6-cga-omipv6-04 (work in progress), May 2005.

[I-D.haddad-privacy-omipv6-anonymity]
Haddad, W., "Anonymity and Unlinkability Extension for CGA-OMIPv6", draft-haddad-privacy-omipv6-anonymity-00 (work in progress), June 2005.

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

9.2 Informative References

[I-D.haddad-momipriv-problem-statement]
Haddad, W., "Privacy for Mobile and Multi-homed Nodes: MoMiPriv Problem Statement", draft-haddad-momipriv-problem-statement-01 (work in progress), February 2005.

[I-D.ietf-mobike-design]
Kivinen, T. and H. Tschofenig, "Design of the MOBIKE

protocol", draft-ietf-mobike-design-02 (work in progress), February 2005.

[I-D.ietf-mobike-protocol]
Eronen, P., "IKEv2 Mobility and Multihoming Protocol (MOBIKE)", draft-ietf-mobike-protocol-00 (work in progress), June 2005.

[I-D.ietf-send-cga]
Aura, T., "Cryptographically Generated Addresses (CGA)", draft-ietf-send-cga-06 (work in progress), April 2004.

Authors' Addresses

Hannes Tschofenig
Siemens
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Email: Hannes.Tschofenig@siemens.com

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

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

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information

on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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