

Network Working Group
Internet-Draft
Expires: April 26, 2007

W. Haddad
S. Krishnan
Ericsson Research
F. Dupont
CELAR
M. Bagnulo
UC3M
H. Tschofenig
Siemens AG
October 23, 2006

**An Anonymity and Unlinkability Extension for OMIPv6
draft-haddad-privacy-omipv6-anonymity-02**

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 April 26, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

The "Optimized Mobile IPv6 with CBA" (OMIPv6) protocol specifies a new route optimization (RO) mechanism, which offers better security,

less signaling messages and reduces the handoff latency. This document describes a new extension to be added to the OMIPv6 protocol in order to provide the anonymity and the unlinkability aspects at the IP layer.

Table of Contents

1.	Introduction	3
2.	Conventions used in this document	4
3.	Glossary	5
4.	Problem Statement	6
5.	Proposed Solution	8
6.	Packet Format	12
7.	Privacy Considerations	14
8.	Security Considerations	15
9.	References	16
9.1.	Normative References	16
9.2.	Informative References	16
	Authors' Addresses	18
	Intellectual Property and Copyright Statements	19

1. Introduction

Optimized Mobile IPv6 [[OMIPv6](#)] 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 or pseudonymity, and unlinkability aspects. Supporting these privacy aspects in OMIPv6 would allow a mobile user to move outside its home network without disclosing its real IPv6 home address nor linking its different moves together, and thereby preventing eavesdroppers from the ability to correlate its actions at the IP layer.

This document describes privacy extensions to the OMIPv6 protocol.

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. 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 significantly 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 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 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 IPv6 Home Address (HoA) and its new current topological location, i.e., disclosed in its IPv6 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 (detailed in [[MIPv6](#)]) under any circumstance(s), since data packets sent by the CN are addressed to the MN's HoA.

However, replacing the real MN's HoA with a static/dynamic pseudo-HoA does not solve the entire privacy problem as described above. In fact, using static/dynamic pseudo-HoA(s) can still allow the eavesdropper to correlate between MN's movements across the Internet, thus easily breaking the unlinkability feature. Such correlation can be accomplished by simply tracing the sequence number carried by each BU 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, learning the MN's HoA can reveal all its pseudo-HoAs 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 with the same pseudo-HoA. In this case, the correlation may also reveal the exact time of the MN's movement(s), regardless of the BU message content.

In addition to the correlation based on tracing data packets only, which provides the possibility to correlate between different movements, another correlation becomes possible between the signaling messages and the data packets. In fact, tracing the BU messages in addition to the data packets can 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) and/or pseudo-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:

- o prevent disclosing the MN's HoA in any BU message.
- o prevent any correlation between BU messages by avoiding using the same pseudo-HoA in more than one BU message.
- o prevent any correlation between the BU messages via the sequence number.
- o prevent any correlation between data packets exchanged with the current CoA and the next BU message sent after performing an IP handover.
- o prevent any correlation between data carried by the BU message and data packets exchanged directly after sending/receiving BU/BA message(s).

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

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:

1. 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 special sequence number handling).
2. replacing the home address inserted in the HAO with an ephemeral identifier.
3. associating the interface identifier (iid) of the MN's home address with the statistically unique cryptographically-Based Identifiers (described in [\[CBID\]](#)).

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 BT mode during the subsequent data packets exchange.

The MN MUST set the "P" bit in the PBU message, regardless of the MN's location (i.e., also if located in its 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 crypto-based identifier (CBID). Note that using the CBID technology in Mobile IPv6 for privacy purposes has been introduced in [\[MIPriv\]](#).

During the initial signaling messages exchange 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 for the initial case, the VHoA is the CBID, thus the value sent in the PBU message is equal to SHA1(CBID)).

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 in the PBT message and sends it to the MN. When the MN gets the PBT message, it sends a BU message carrying the "P" bit, the challenge and the real CBID (i.e., the CBID is inserted in 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:

$$\text{iid}(\text{CoA}) = \text{First}(64, \text{SHA1}(\text{CBID}))$$

Where:

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

Upon receiving the first BU message with the "P" bit set, the CN starts by checking its validity, which is done by hashing the content of the HAO, i.e., the CBID, and comparing 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 BU message. The third step after a successful validation would be to create an entry in the BCE for the MN's VHoA and CoA. The CN MUST also generate a long lifetime shared secret (i.e., SKbm) and sends it to the MN in the BA message as described in [\[OMIPv6\]](#).

The presence of the "P" bit in the BU message serves another purpose, which is to request the CN to replace the sequence number carried by the BU message, in its BCE with the "next" value, i.e., the value 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 increase the 32-bit sequence number value. When the privacy extensions introduced in this document are used, then both endpoints MUST increment the SQV with a constant value equal to the one obtained from hashing the SKbm. Finally, the increased 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:

$$\text{Khbm} = \text{SHA1}(\text{SKbm})$$
$$\text{nSQV} = \text{First}(32, \text{SHA1}((\text{pSQV}) \mid \text{Khbm}))$$

Where:

- o SKbm is a long lifetime binding management key
- o Khbm is the hashed binding management key
- o pSQV is the previous SQV, i.e., SQV sent in the last BU message sent by the MN and already processed by the CN.
- o nSQV is the hash 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 or updating the MN's corresponding 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 each a different 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 pair of addresses (CoA, VHoA) to be used in the data packets exchange following the BCE creation or 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)

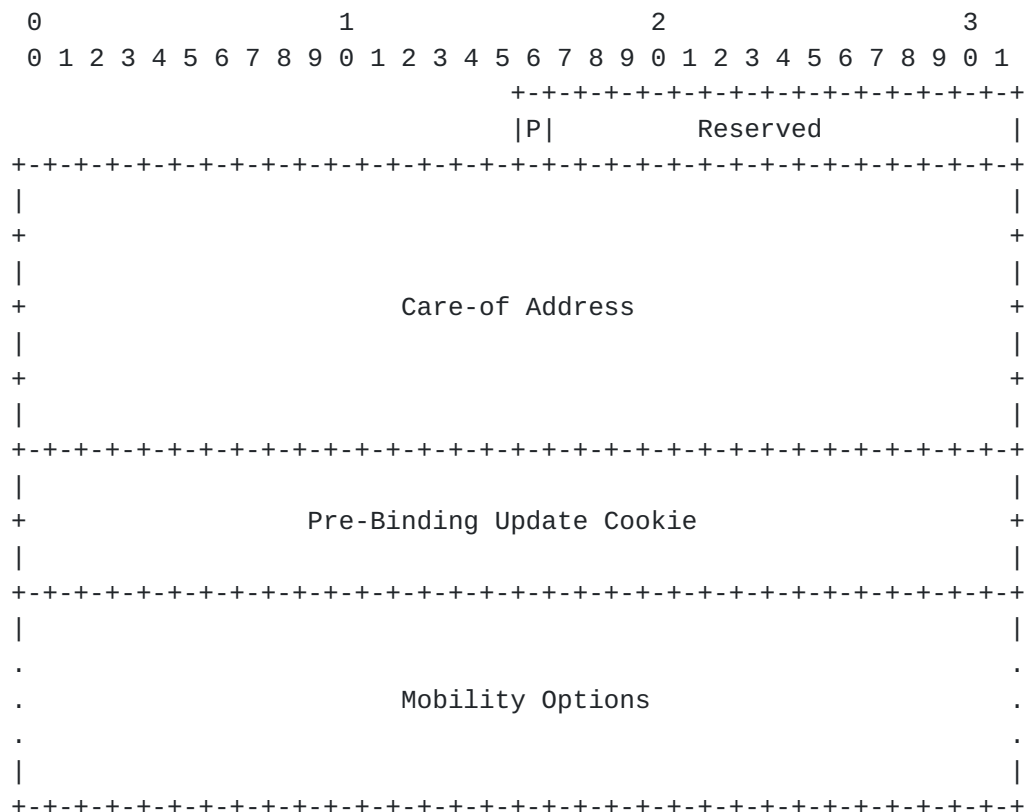
Where:

- o nCoA is the MN's care-of address sent in the BU message.
- o 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 [\[HBA\]](#)). As mentioned above, 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.

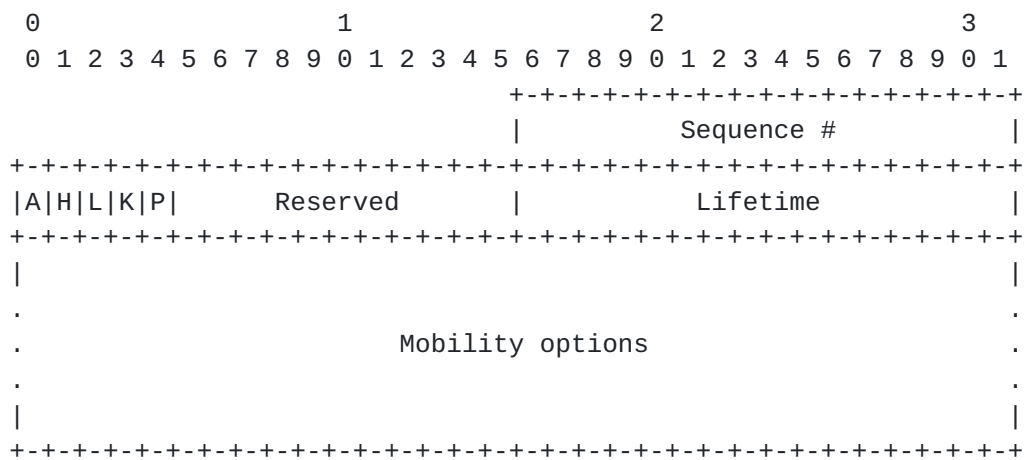
When the MN sends a BU message carrying the "P" bit, the SQV MUST be used alone by the CN to detect the presence of an entry corresponding to the MN in its BCE. If an entry containing the same SQV is found,

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



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 [[MIPv6-IKE](#)] and [[MIPv6-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 tightly 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 existing 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. References

9.1. Normative References

- [MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [MIPv6-IKE]
Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", [RFC 3776](#), June 2004.
- [MIPv6-IKEv2]
Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", Internet Draft, [draft-ietf-mip6-ikev2-ipsec-06.txt](#), April 2006.
- [OMIPv6] Arkko, J., Vogt, C., and W. Haddad, "Applying Cryptographically Generated Addresses and Credit-Based Authorization to Optimize Mobile IPv6 (OMIPv6)", Internet Draft, [draft-ietf-mipshop-omipv6-cga-cba-01](#), September 2006.
- [TERM] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", [RFC 2119](#), BCP , March 1997.

9.2. Informative References

- [ANON] Pfitzmann et al., A., "Anonymity, Unobservability, Pseudonymity and Identity Management - A Consolidated Proposal for Terminology", Anon Terminology Draft v0.28, May 2006.
- [CBID] Montenegro, G. and C. Castelluccia, "Cryptographically-Based Identifiers (CBID): Concepts and Applications", ACM Transactions on Information and System Security TISSEC, February 2004.
- [HBA] Bagnulo, M., "Hash Based Addresses (HBA)", Internet Draft, [draft-ietf-shim6-hba-02.txt](#), October 2006.
- [MIPriv] Castelluccia, C., Dupont, F., and G. Montenegro, "A Simple Privacy Extension for Mobile IPv6", Internet Draft, [draft-dupont-mip6-privacyext-04.txt](#), July 2006.
- [MOMIPRIV]
Haddad, W., Nordmark, E., Dupont, F., Bagnulo, M., Park, S., and B. Patil, "Privacy for Mobile and Multi-homed

Nodes: MoMiPriv Problem Statement", Internet-Draft, [draft-haddad-momipriv-problem-statement-03.txt](#), June 2006.

[PRIVACY] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", Internet-Draft, [draft-ietf-ipv6-privacy-address-v2-05.txt](#), August 2006.

Authors' Addresses

Wassim Haddad
Ericsson Research
Torshamnsgatan 23
SE-164 80 Stockholm
Sweden

Phone: +46 8 4044079
Email: Wassim.Haddad@ericsson.com

Suresh Krishnan
Ericsson Research
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900
Email: Suresh.Krishnan@ericsson.com

Francis Dupont
CELAR

Email: Francis.Dupont@point6.net

Marcelo Bagnulo
UC3M
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
Spain

Phone: +31 91 6249500
Email: 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

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 (2006). 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.

