Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 15, 2009

A. Patel
K. Leung
Cisco Systems
M. Khalil
H. Akhtar
Nortel Networks
K. Chowdhury
Starent Networks
July 14, 2008

Authentication Protocol for Mobile IPv6
draft-ietf-mip6-rfc4285bis-03.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 15, 2009.

Abstract

IPsec is specified as the means of securing signaling messages between the Mobile Node and Home Agent for Mobile IPv6. Mobile IPv6 signalling messages that are secured include the Binding Updates and Acknowledgement messages used for managing the bindings between a Mobile Node and its Home Agent. This document proposes an alternate method for securing Mobile IPv6 signaling messages between a Mobile Nodes and Home Agents. The alternate method defined here consists of a Mobile IPv6 specific authentication option that can be added to Mobile IPv6 signalling messages.

Table of Contents

1. Introduction

The base Mobile IPv6 (MIPv6) specification [RFC3775] specifies the signaling messages, Binding Update (BU) and Binding Acknowledgement (BA), between the Mobile Node (MN) and Home agent (HA) to be secured by the IPsec Security Associations (IPsec SAs) that are established between these two entities.

This document proposes a solution for securing the Binding Update and Binding Acknowledgment messages between the Mobile Node and Home agent using an authentication option which is included in these messages. Such a mechanism enables IPv6 mobility in a host without having to establish an IPsec SA with its Home Agent. A Mobile Node can implement Mobile IPv6 without having to integrate it with the IPsec module, in which case the Binding Update and Binding Acknowldegement messages (between MN and HA) are secured with the authentication option.

The authentication mechanism proposed here is similar to the authentication mechanism used in Mobile IPv4 [RFC3344].

1.1. Applicability Statement

The authentication option specified in Section 5 is applicable in certain types of networks that have the following characteristics:

- Networks in which the authentication of the MN for network access is done by an authentication server in the home network via the home agent. The security association is established by the network operator (provisioning methods) between the MN and a backend authentication server (eg. home AAA server). MIPv6 as per RFC3775/ 3776 relies on the IPsec SA between the MN and an HA. In cases where the assignment of the HA is dynamic and the only static or long term SA is between the MN and a backend authentication server, the authentication option is desirable.

- In certain deployment environments, the Mobile Node needs dynamic assignment of a home agent and home address. The assignment of such can be on a per session basis or on a per MN power-up basis. In such scenarios, the MN relies on an identity such as an NAI [RFC4283], and a security association with a AAA server to obtain such bootstrapping information. The security association is created via an out-of-band mechanism or by non Mobile IPv6 signaling. The out-of-band mechanism can be specific to the deployment environment of a network operator. In cdma2000 network deployments this information can be obtained at the time of network access authentication via [3GPP2] specific extensions to PPP or DHCPv6 on the access link and by AAA extensions in the core. It should be noted that the out-of-band mechanism if

not within the scope of the authentication option Section 5 and hence not described therein.

- Network deployments in which not all Mobile Nodes and home agents have Internet Key Exchange verion 2 (IKEv2) implementations and support for the integration of IKEv2 with backend AAA infrastructures. IKEv2 as a technology has yet to reach maturity status and widespread implementations needed for commercial deployments on a large scale.

- Networks which expressly rely on the backend AAA infrastructure as the primary means for identifying and authentication/authorizing a mobile user for MIPv6 service.

- Networks in which the establishment of the security association between the mobile node and the authentication server (home AAA server) is established using an out-of-band mechanism and not by any key exchange protocol. Such networks will also rely on out-of-band mechanisms to renew the security association (between MN and home AAA server) when needed.

- Networks which are bandwidth constrained (such as cellular wireless networks) and there exists a strong desire to minimize the number of signaling messages sent over such interfaces. MIPv6 signaling which relies on IKE as the primary means for setting up an SA between the MN and HA requires more signaling messages compared with the use of an authentication option carried in the BU/BA messages.

One such example of networks that have such characteristics are cdma networks as defined in [3GPP2].

2. Overview

This document presents a lightweight mechanism to authenticate the Mobile Node at the Home Agent or at the Authentication, Authorization and Accounting (AAA) server in Home network (HAAA) based on a shared-key based mobility security association between the Mobile Node and the respective authenticating entity. This shared-key based mobility security association (shared-key based mobility SA) may be statically provisioned or dynamically created. The term "mobility security association" referred to in this document is understood to be a "shared-key based Mobile IPv6 authentication" security association.

This document introduces new mobility options to aid in authentication of the Mobile Node to the Home Agent or home AAA server. The confidentiality protection of Return Routability messages and authentication/integrity protection of Mobile Prefix Discovery (MPD) is not provided when these options are used for authentication of the Mobile Node to the Home Agent. Thus, unless the network can guarantee such protection (for instance, like in 3GPP2 networks), Route Optimization and Mobile Prefix Discovery should not be used when using the authentication option.

3. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

3.1. General Terms

First (size, input)

Some formulas in this specification use a functional form "First (size, input)" to indicate truncation of the "input" data so that only the first "size" bits remain to be used.

Shared-key based Mobility Security Association

Security relation between Mobile Node and its Home Agent, used to authenticate the Mobile Node for mobility service. The shared-key based mobility security association between Mobile Node and Home Agent consists of a mobility SPI, a shared-key, an authentication algorithm and the replay protection mechanism in use.

Mobility Security Pamater Index (SPI)

A number in the range [0-4294967296] used to index into the shared-key based mobility security associations. The SPI value can be same or different from MN to HA and from HA to MN in relation to MN-HA authentication mobility option. Value range [0-255] is reserved.

4. Operational flow

The figure below describes the sequence of messages sent and received between the MN and HA in the registration process. Binding Update (BU) and Binding Acknowledgement (BA) messages are used in the registration process.

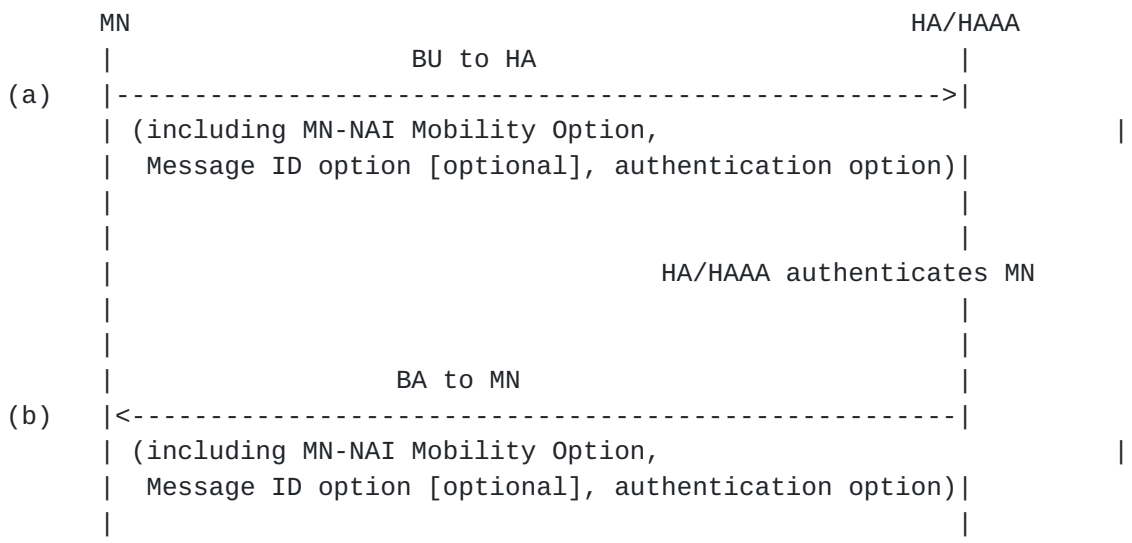

Figure 1: Home Registration with Authentication Protocol

The Mobile Node MUST include the MN-NAI Mobility Option, as defined in [RFC4283] to identify itself while authenticating with the Home Agent.

Mobile Node MAY use Message Identifier option as defined in Section 6 for additional replay protection.

The authentication option described in Section 5 may be used by the mobile node to transfer authentication data when the mobile node and the home agent are utilizing a mobility SPI (a number in the range [0-4294967296] used to index into the shared-key based mobility security associations).

5. Mobility message authentication option

This section defines a message authentication mobility option that may be used to secure Binding Update and Binding Acknowledgement messages. This option can be used along with IPsec or preferably as an alternate mechanism to authenticate Binding Update and Binding Acknowledgement messages in the absence of IPsec.

This document also defines subtype numbers, which identify the mode of authentication and the peer entity to authenticate the message. Two subtype numbers are specified in this document. Other subtypes may be defined for use in the future.

Only one instance of an authentication option of a particular subtype can be present in the message. One message may contain multiple instances of authentication options with different subtype values. If both Mobile Node to Home Agent (MN-HA) and Mobile Node to Authentication Authorization Accounting server (MN-AAA) authentication mobility options are present, the MN-HA authentication option MUST be present before the MN-AAA authentication option (else, the HA MUST discard the message).

When a Binding Update or Binding Acknowledgement is received without an authentication option and the entity receiving it is configured to use authentication option or has the shared-key based mobility security association for authentication option, the entity should silently discard the received message.

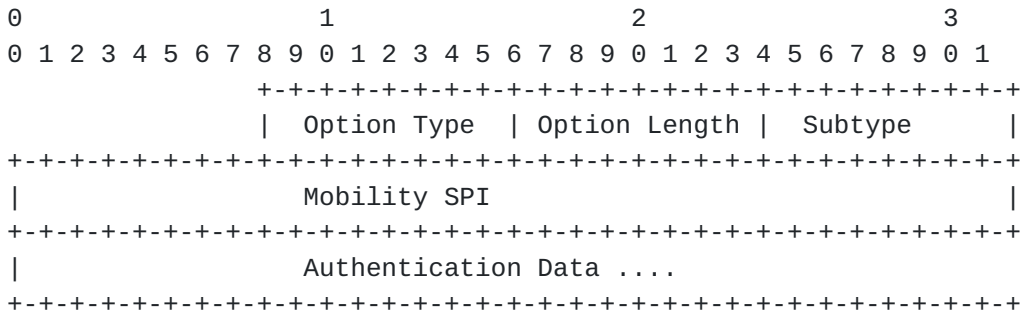

Figure 2

Option Type:

AUTH-OPTION-TYPE to be defined by IANA. An 8-bit identifier of the type mobility option.

Option Length:

8-bit unsigned integer, representing the length in octets of the Sub-type, mobility SPI and Authentication Data fields.

Subtype:

A number assigned to identify the entity and/or mechanism to be used to authenticate the message.

Mobility SPI:

Mobility Security Parameter Index

Authentication Data:

This field has the information to authenticate the relevant mobility entity. This protects the message beginning at the Mobility Header upto and including the mobility SPI field.

Alignment requirements :

The alignment requirement for this option is 4n + 1.

5.1. MN-HA authentication mobility option

The format of the MN-HA authentication mobility option is as defined in Figure 2. This option uses the subtype value of 1. The MN-HA authentication mobility option is used to authenticate the Binding Update and Binding Acknowledgement messages based on the shared-key based security association between the Mobile Node and the Home Agent.

The shared-key based mobility security association between Mobile Node and Home Agent used within this specification consists of a mobility SPI, a key, an authentication algorithm and the replay protection mechanism in use. The mobility SPI is a number in range [0-4294967296], where the range [0-255] is reserved. In particular, the SPI selects the authentication algorithm and shared key used in computing the Authenticator. In order to ensure interoperability, an implementation MUST be able to associate any SPI value with any authentication algorithm. In addition, all implementations MUST implement the default authentication algorithm, HMAC_SHA1. Other algorithms are allowed but are not specified in this document. The shared-key consists of an arbitrary value and is 20 octets in length.

The replay protection mechanism may use the sequence number as specified in [RFC3775] or the Timestamp option as defined in Section 6. If the Timestamp option is used for replay protection as defined in Section 6, the mobility security association includes a "close enough" field to account for clock drift. A default value of 7 seconds SHOULD be used. This value SHOULD be greater than 3 seconds.

The MN-HA authentication mobility option MUST be the last option in a message with mobility header if it is the only authentication option in the message.

The authentication data is calculated on the message starting from the mobility header upto and including the mobility SPI value of this option.

Authentication Data = First (96, HMAC_SHA1(MN-HA Shared key, Mobility Data))

Mobility Data = care-of address | home address | Mobility Header(MH) Data

MH Data is the content of the Mobility Header upto and including the mobility SPI field of the Mobility message authentication option. The Checksum field in Mobility Header MUST be set to 0 to calculate the Mobility Data.

5.1.1. Processing Considerations

The assumption is that Mobile Node has a shared-key based security association with the Home Agent. The Mobile Node MUST include this option in a BU if it has a shared-key based mobility security association with the Home Agent. The Home Agent MUST include this option in the BA if it received this option in the corresponding BU and Home Agent has a shared-key based mobility security association with the Mobile Node.

The Mobile Node or Home Agent receiving this option MUST verify the authentication data in the option. If authentication fails, the Home Agent MUST send BA with Status Code MIPV6-AUTH-FAIL. If the Home Agent does not have shared-key based mobility SA, Home Agent MUST discard the BU. The Home Agent MAY log such events.

5.2. MN-AAA authentication mobility option

The format of the MN-AAA authentication mobility option is as defined in Figure 2. This option uses the subtype value of 2. The MN-AAA authentication mobility option is used to authenticate the Binding Update message based on the shared mobility security association between Mobile Node and AAA server in Home network (HAAA). It is not used in Binding Acknowledgement messages. The corresponding Binding Acknowledgement messages must be authenticated using the MN-HA authentication option Section 5.1.

This must be the last option in a message with mobility header. The corresponding response MUST include the MN-HA Authentication option, and MUST NOT include the MN-AAA Authentication option.

The Mobile Node MAY use Mobile Node Identifier option [RFC4283] to enable the Home Agent to make use of available AAA infrastructure.

The authentication data is calculated on the message starting from the mobility header upto and including the mobility SPI value of this option.

The authentication data shall be calculated as follows:

Authentication data = hash_fn(MN-AAA Shared key, MAC_Mobility Data)

hash_fn() is decided by the value of mobility SPI field in the authentication option.

SPI = HMAC_SHA1_SPI:

If mobility SPI has the well-known value HMAC_SHA1_SPI, then

hash_fn() is HMAC_SHA1. When HMAC_SHA1_SPI is used, the BU is authenticated by AAA using HMAC_SHA1 authentication. In that case, MAC_Mobility Data is calculated as follows:

MAC_Mobility Data = SHA1(care-of address | home address | MH Data)

MH Data is the content of the Mobility Header upto and including the mobility SPI field of this option.

5.2.1. Processing Considerations

The use of the MN-AAA authentication option assumes that AAA entities at the home site communicate with the HA via an authenticated channel. Specifically, a BU with the MN-AAA authentication option is authenticated via a home AAA server. The specific details of the interaction between the HA and the AAA server is beyond the scope of this document.

When the Home Agent receives a Binding Update with the MN-AAA authentication option, the Binding Update is authenticated by an entity external to the Home Agent, typically a AAA server.

5.3. Authentication Failure Detection at the Mobile Node

In case of authentication failure, the Home Agent MUST send a Binding Acknowledgement with status code MIPV6-AUTH-FAIL to the Mobile Node, if a shared-key based mobility security association to be used between Mobile Node and Home Agent for authentication exists. If there is no shared-key based mobility security association, HA MUST silently discard the Binding Update. HA may log the message for administrative action.

Upon receiving a Binding Acknowledgement with status code MIPV6-AUTH-FAIL, the Mobile Node SHOULD stop sending new Binding Updates to the Home Agent.

6. Mobility message replay protection option

The Mobility message replay protection option MAY be used in Binding Update/Binding Acknowledgement messages when authenticated using the mobility message authentication option as described in Section 5.

The mobility message replay protection option is used to let the Home Agent verify that a Binding Update has been freshly generated by the Mobile Node and not replayed by an attacker from some previous Binding Update. This is especially useful for cases where the Home Agent does not maintain stateful information about the Mobile Node after the binding cache entry has been removed. The Home Agent does the replay protection check after the Binding Update has been authenticated. The mobility message replay protection option when included is used by the Mobile Node for matching BA with BU.

If this mode of replay protection is used, it needs to be part of the shared-key based mobility security association.

If the policy at Home Agent mandates replay protection using this option (as opposed to the sequence number in Mobility Header in Binding Update) and the Binding Update from Mobile Node does not include this option, Home Agent discards the BU and sets the Status Code in BA to MIPV6-MESG-ID-REQD.

When the Home Agent receives the mobility message replay protection option in Binding Update, it MUST include the mobility message replay protection option in Binding Acknowledgement. Appendix A provides details regarding why the mobility message replay protection option MAY be used when using the authentication option.

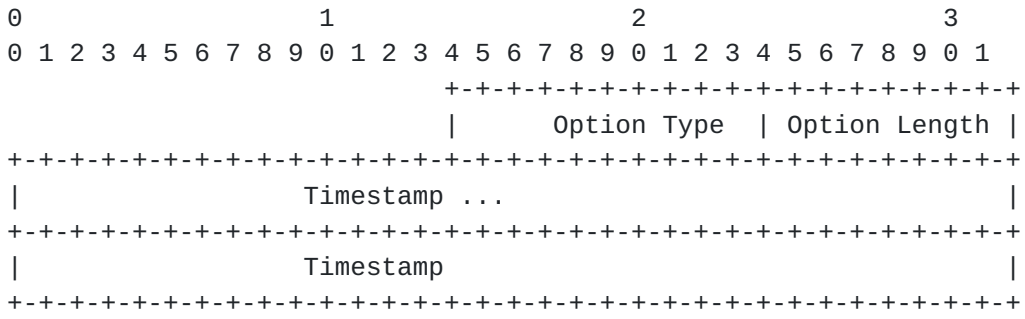

Figure 3

Option Type:

MESG-ID-OPTION-TYPE to be defined by IANA. An 8-bit identifier of the type mobility option.

Option Length:

8-bit unsigned integer, representing the length in octets of the Timestamp field.

Timestamp:

This field carries the 64 bit timestamp.

Alignment requirements :

The alignment requirement for this option is 8n + 2.

The basic principle of timestamp replay protection is that the node generating a message inserts the current time of day, and the node receiving the message checks that this timestamp is sufficiently close to its own time of day. Unless specified differently in the shared-key based mobility security association between the nodes, a default value of 7 seconds MAY be used to limit the time difference. This value SHOULD be greater than 3 seconds. The two nodes must have adequately synchronized time-of-day clocks.

The Mobile Node MUST set the Timestamp field to a 64-bit value formatted as specified by the Network Time Protocol [RFC1305]. The low-order 32 bits of the NTP format represent fractional seconds, and those bits which are not available from a time source SHOULD be generated from a good source of randomness. Note, however, that when using timestamps, the 64-bit Timestamp used in a Binding Update from the Mobile Node MUST be greater than that used in any previous

successful Binding Update.

After successful authentication of Binding Update (either locally at the Home Agent or when a success indication is received from the AAA server), the Home Agent MUST check the Timestamp field for validity. In order to be valid, the timestamp contained in the Timestamp field MUST be close enough to the Home Agent's time of day clock and the timestamp MUST be greater than all previously accepted timestamps for the requesting Mobile Node.

If the timestamp is valid, the Home Agent copies the entire Timestamp field into the Timestamp field in the BA it returns to the Mobile Node. If the timestamp is not valid, the Home Agent copies only the low-order 32 bits into the BA, and supplies the high-order 32 bits from its own time of day.

If the timestamp field is not valid but the authentication of the BU succeeds, Home Agent MUST send a Binding Acknowledgement with status code MIPV6-ID-MISMATCH. The Home Agent does not create a binding cache entry if the timestamp check fails.

If the Mobile Node receives a Binding Acknowledgement with the code MIPV6-ID-MISMATCH, the Mobile Node MUST authenticate the BA by processing the MN-HA authentication mobility option.

If authentication succeeds, the Mobile Node MUST adjust its timestamp and send subsequent Binding Update using the updated value.

Upon receiving a BA that does not contain the MIPV6-ID-MISMATCH status code, the Mobile Node MUST compare the Timestamp value in the BA to the Timestamp value it sent in the corresponding BU. If the values match, the Mobile Node proceeds to process the MN-HA authentication data in the BA. If the values do not match, the Mobile Node silently discards the BA.

7. Security Considerations

This document proposes new authentication options to authenticate the control message between Mobile Node, Home Agent and/or home AAA (as an alternative to IPsec). The new options provide for authentication of Binding Update and Binding Acknowledgement messages. The MN-AAA authentication options provides for authentication with AAA infrastructure.

This specification also introduces an optional replay protection mechanism in Section 6, to prevent replay attacks. The sequence number field in the Binding Update is not used if this mechanism is used. This memo defines the timestamp option to be used for mobility message replay protection.

8. IANA Considerations

IANA services are required for this specification. The values for new mobility options and status codes must be assigned from the Mobile IPv6 [RFC3775] numbering space.

The values for Mobility Option types AUTH-OPTION-TYPE and MESG-ID-OPTION-TYPE, as defined in Section 5 and Section 6 need to be assigned. The suggested values are 8 for the AUTH-OPTION-TYPE and 9 for the MESG-ID-OPTION-TYPE Mobility Option.

The values for status codes MIPV6-ID-MISMATCH, MIPv6-AUTH-FAIL and MIPV6-MESG-ID-REQD as defined in Section 6, Section 6 and Section 5.3 also need to be assigned. The suggested values are 144 for MIPV6-ID-MISMATCH 145 for MIPV6-MESG-ID-REQD and 146 for MIPV6-AUTH-FAIL.

IANA should record values for these new Mobility Options and the new Status Codes.

A new section for enumerating algorithms identified by specific mobility SPIs within the range 0-255 is to be added to

http://www.isi.edu/in-notes/iana/assignments/mobility-parameters

The currently defined values are as follows:

The value 0 should not be assigned.

The value 3 is suggested for HMAC_SHA1_SPI as defined in Section 5.2.

The value 5 is reserved for use by 3GPP2.

New values for this namespace can be allocated using IETF Consensus. [RFC2434].

In addition, IANA needs to create a new namespace for the subtype field of the MN-HA and MN-AAA authentication mobility options under

http://www.isi.edu/in-notes/iana/assignments/mobility-parameters

The currently allocated values are as follows:

1 MN-HA authentication mobility option Section 5.1

2 MN-AAA authentication mobility option Section 5.2

New values for this namespace can be allocated using IETF Consensus. [RFC2434].

9. Acknowledgements

The authors would like to thank Basavaraj Patil, Charlie Perkins Vijay Devarapalli, Jari Arkko and Gopal Dommety for their thorough review and suggestions on the document. The authors would like to acknowledge the fact that a similar authentication method was considered in base protocol [RFC3775] at one time. Many thanks to Hannes Tschofenig and Jouni Korhonen for their detailed review and comments.

10. References

10.1. Normative References

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

10.2. Informative References

[3GPP2] "cdma2000 Wireless IP Network Standard", 3GPP2 X.S0011-D, September 2005.

[whyauth] Patil et. al., B., "Why Authentication Data suboption is needed for MIPv6", draft-ietf-mip6-whyauthdataoption-06.txt (work in progress), July 2008.

Appendix A. Rationale for mobility message replay protection option

Mobile IPv6 [RFC3775] defines a Sequence Number in the mobility header to prevent replay attacks. There are two aspects that stand out in regards to using the Sequence Number to prevent replay attacks.

Firstly, the specification states that Home Agent should accept a BU with a Sequence Number greater than the Sequence Number from previous Binding Update. This implicitly assumes that the Home Agent has some information regarding the Sequence Number from previous BU (even when the binding cache entry is not present). Secondly, the specification states that if the Home Agent has no binding cache entry for the indicated home address, it MUST accept any Sequence Number value in a received Binding Update from this Mobile Node.

With the mechanism defined in this draft, it is possible for the Mobile Node to register with a different Home Agent during each mobility session. Thus, it is unreasonable to expect each Home Agent in the network to maintain state about the Mobile Node. Also, if the Home Agent does not cache information regarding sequence number, as per the second point above, a replayed BU can cause a Home Agent to create a binding cache entry for the Mobile Node. Thus, when authentication option is used, Sequence Number does not provide protection against replay attack.

One solution to this problem (when Home Agent does not save state information for every Mobile Node) would be for the Home Agent to reject the first BU and assign a (randomly generated) starting sequence number for the session and force the Mobile Node to send a fresh BU with the suggested sequence number. While this would work in most cases, it would require an additional round trip and this extra signalling and latency is not acceptable in certain deployments [3GPP2]. Also, this rejection and using sequence number as a nonce in rejection is a new behavior that is not specified in [RFC3775].

Thus, this specification uses the mobility message replay protection option to prevent replay attacks. Specifically, timestamps are used to prevent replay attacks as described in Section 6.

It is important to note that as per Mobile IPv6 [RFC3775] this problem with sequence number exists. Since the base specification mandates the use of IPsec (and naturally that goes with IKE in most cases), the real replay protection is provided by IPsec/IKE. In case of BU/BA between Mobile Node and CN, the liveness proof is provided by the use of nonces which the CN generates.

Appendix B. Change Log

B.1. Key length change

Changed the key length to 20 octets from 16 octets in section Section 5.1

B.2. Changed IKEv2 draft number to RFC

In the reference section.

B.3. Text removed in applicability statement

Removed IKEv2 related text in section Section 1.1

Authors' Addresses

Alpesh Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US

Phone: +1 919-392-5626
Email: alpesh@cisco.com

Kent Leung
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US

Phone: +1 408-526-5030
Email: kleung@cisco.com

Mohamed Khalil
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US

Phone: +1 972-685-0574
Email: mkhalil@nortel.com

Haseeb Akhtar
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US

Phone: +1 972-684-4732
Email: haseebak@nortel.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
US

Phone: +1 214-547-7307
Email: kchowdhury@starentnetworks.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

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.

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, THE IETF TRUST 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.

Intellectual Property

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.