HA-AAA Diameter interface for MIPv6

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, 2007.

Abstract

This document specifies a Diameter application between AAAH and HA that allows authentication, authorization and accounting for Mobile IPv6 services. Further, this interface could also be used for bootstrapping of MIPv6.

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 RFC 2119 [8].
1. Introduction

MIPv6 allows a mobile node to change its point of attachment which is recognized by CoA while maintaining fixed home address. This is achieved by sending binding Update to Home agent. It is necessary to provide the authentication for MIPv6 messages. [2] discusses use of IPsec to provide the authentication but during recent times mechanisms based on MIPv4 have become popular in MIPv6 [1]. In this draft we provide a Diameter MIPv6 application to AAA functionality for MIPv6.

1.1 Mobility Security Associations

MIPv6 [2] assumes the existence of a Mobility Security Association (MSA) between the MN and HA (MN-HA MSA). The MN-HA MSA is used to authenticate the binding Updates from the MN to the HA. It is important to perform the authentication for binding update message. The threat model for MIPv6 is discussed in [2]. MN-HA MSA is used to calculate MN-HA mobility message authentication option as discussed in [1]. MN-HA MSA is allocated typically by AAAH. Authentication of the MN for MIPv6 service is required before MN-HA MSA is allocated to MN. This requires another security association MN-AAA MSA to exist between MN and AAAH. This MSA is provisioned at the MN when it
subscribes for MIPv6 service. For security purpose MN can have multiple MN-AAA MSAs provisioned and it could randomly choose one of them for interaction with AAAH. MN-AAA MSA is also useful if the authentication at HA fails and AAAH is required to authenticate and allocate new MN-HA MSA.

2.
Scenarios

MN request MIPv6 service by sending a BU to HA. If MN do not have MN-HA MSA then it MUST include the MN-AAA authentication option and the MN-HA key gen req [7]. Since the HA does not have a SA established with MN, it cannot locally authenticate MN for MIPv6 service. HA sends MHQ to AAAH and it includes the part of BU which was used to calculate HMAC in MN-AAA mobility message authentication option as explained in [1]. It MUST send MN-AAA mobility message authentication option as a separate AVP. This makes AAAH agnostic of the MIP message format. AAAH authenticates BU and sends the reply with MHI message. Mobile Node can also request for a Home IP address by adding the option explained in [7]. HA or AAAH depending on IP management mechanism can allocate the IPv6 address once MN authentication is successful. HA stores the MN-HA MSA locally and sends the key generation information necessary to MN in BA [7]. Key in MN-HA MSA is not sent to MN. Figure 1 explains the scenario

2.1
Renewal of MN-HA MSA

MN MUST renew the MN-HA MSA before its lifetime expires. This is done by sending a BU with MN-HA-key gen request [7] and MN-HA Mobility

---BU+ mn-aaa--->
auth option

<---BA+bootstrap--
info

-----BU+ mn-aaa--->
auth option

-----MHQ --------->
<----MHI ---------

Figure 1. Authentication for MIPv6

MN-HA MSA

MN

Vishnu et. al Expires April 2007 [Page 3]
Message Authentication Option. HA authenticates the BU and creates MHQ to get the new MN-HA MSA from AAAH. since the HA was able to authenticate the BU, it SHOULD not send the BU to AAAH for authentication. Figure 2 explains the scenario.

```
MN       HA       MSA
| ----BU+ mn-ha---->|
| auth option      |
| ----MHQ -------->|
| <----MHI --------|
| <---BA+ new msa --|
```

Figure 2. Renewal of MN-HA MSA

2.2

HA discovery

When MN powers up in the foreign network it may not have information about HA’s IP address. In this draft we assume that MN performs HA discovery mechanism. HA discovery mechanisms are discussed in [2]. DNS can also be used to acquire HA’s IP address.

3. Diameter Protocol Considerations

This section details the relationship of the Diameter Mobile IPv6 application to the Diameter base protocol.

This document specifies Diameter Application-ID TBD. Diameter nodes conforming to this specification MAY advertise support by including the value of TBD in the Auth-Application-Id or the Acct- Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands [5]. The value of TBD MUST be used as the Application-Id in all MHQ/MHI commands.

3.1

Command-Code Values

This section defines Command-Code [5] values that MUST be supported by all Diameter implementations conforming to this specification. The following Command Codes are defined in this specification.

<table>
<thead>
<tr>
<th>Command-Name</th>
<th>Abbreviation</th>
<th>Code</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIPv6-Home-Agent-Query</td>
<td>MHQ</td>
<td>TBD</td>
<td>3.2</td>
</tr>
</tbody>
</table>

Vishnu et. al Expires April 2007 [Page 4]
3.2 MIPv6-Home-Agent-Query (MHQ)

HA sends the MIPv6-Home-Agent-Query, indicated by the Command-Code field set to TBD and the ‘R’ bit set in the Command Flags field, to the AAAH. When session keys are requested for use by the mobile node, the AAAH MUST create them and include them in the MHI message.

Message Format

< MIPv6-Home-Agent-Query > ::= < Diameter Header: TBD, REQ, PXY >
  < Session-Id >
  { Auth-Application-Id }
  { Origin-Host }
  { Origin-Realm }
  { User-Name }
  { Destination-Realm }
  [ MIP-binding-update ]
  [ MN-AAA Authenticator info ]
  [ HoA ]
  [ CoA ]
  [ Destination-Host ]
  [ Origin-State-Id ]
  * [ Proxy-Info ]
  * [ Route-Record ]
  * [ AVP ]

3.3 MIPv6-Home-Agent-Information (MHI)

AAAH sends the MIPv6-Home-Agent-Information (MHI), indicated by the Command-Code field set to TBD and the ‘R’ bit cleared in the Command Flags field, to the Home Agent.

Message Format

< Home-Agent-MIP-Information > ::= < Diameter Header: TBD, PXY >
  < Session-Id >
  { Auth-Application-Id }
  { Result-Code }
  { Origin-Host }
  { Origin-Realm }
  { Destination-Realm }
  { User-Name }
  { Destination-Host }
  { MIP-MN-to-HA-MSA }
  * [ Proxy-Info ]
  * [ Route-Record ]
  * [ AVP ]
4. AVP Description

The following table describes the Diameter AVPs defined in the Mobile IPv4 application; their AVP Code values, types, and possible flag values; and whether the AVP MAY be encrypted.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Code Defined</th>
<th>Value Type</th>
<th>MUST</th>
<th>MAY</th>
<th>NOT</th>
<th>NOT</th>
<th>Encr</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIP-binding-update</td>
<td>TBD 4.1</td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>MN-AAA Authenticator info</td>
<td>TBD 4.2</td>
<td>grouped</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>MIP-MN-to-HA-MSA</td>
<td>TBD 4.7</td>
<td>grouped</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>HoA</td>
<td>TBD 4.5</td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
<tr>
<td>CoA</td>
<td>TBD 4.6</td>
<td>OctetString</td>
<td>M</td>
<td>P</td>
<td></td>
<td>V</td>
<td>Y</td>
</tr>
</tbody>
</table>

4.1 MIP-binding-update AVP

The MIP-binding-update AVP is (AVP code TBD) is of type octetstring and contains the modified binding update message. Binding update is modified so that only the portion of BU which is used to calculate HMAC in MN-AAA mobility message authentication option is sent in this AVP.

4.2 MN-AAA Authenticator info AVP

The MN-AAA Authenticator info AVP is (AVP code TBD) is of type grouped and contains MN-AAA Authenticator HMAC and MN-AAA-SPI. Its value has the following ABNF grammar:

```
MN-AAA Authenticator info ::= < AVP Header: TBD >
{ MN-AAA Authenticator HMAC }
{ MN-AAA-SPI }
```

4.3 MN-AAA Authenticator HMAC AVP

The MN-AAA Authenticator HMAC AVP is (AVP code TBD) is of type octetstring and contains the HMAC in the MN-AAA mobility message authentication option in BU message received from MN. AAAH uses MN-AAA MSA and calculates HMAC on the data received in MIP-binding-update AVP and verifies with the data received in MN-AAA Authenticator HMAC AVP. If both the HMACs are same then the authentication is successful.
4.4 MN-AAA-SPI AVP

The MN-AAA SPI AVP is (AVP code TBD) is of type unsigned32 and contains the SPI of the MN-AAA MSA which is used to calculate MN-AAA mobility message authentication option.

4.5 HoA AVP

The HoA AVP is (AVP code TBD) is of type octetstring and contains the Home IPv6 address of the MN. HoA is used to calculate hmac at AAAH and verify it with the received hmac [1].

4.6 CoA AVP

The CoA AVP is (AVP code TBD) is of type octetstring and contains the Care of IPv6 address of the MN. CoA is used to calculate hmac at AAAH and verify it with the received hmac [1].

4.7 MIP-MN-to-HA-MSA AVP

MIP-MN-to-HA-MSA AVP is (AVP code TBD) is of type Grouped and contains the MN-HA MSA. MIP-MN-to-HA-MSA info ::= < AVP Header: TBD >

{ MN-HA-Nonce }
{ MN-HA-SPI }
{ MN-Replay-Mode }
{ MN-HA-Key }
{ MN-HA-MSA-Lifetime }

4.8 MN-HA-Nonce AVP

The MN-HA-Nonce AVP (AVP Code TBD) is of type OctetString and contains the nonce sent to the mobile node for the MN-HA MSA. The mobile node follows the procedures in [1] to generate the key. The AAAH selects the nonce.

4.9 MN-HA-SPI AVP

The MN-HA-SPI AVP (AVP Code TBD) is of type Unsigned32, and it contains the Security Parameter Index the HA that and MN use to refer to the MN-HA MSA.

4.10 MN-Replay-Mode AVP

The MN-Replay-Mode AVP (AVP Code TBD) is of type Enumerated and contains the replay mode the Home Agent for authenticating the mobile node. The AAAH selects the replay mode.
The following values are supported

1. None
2. Timestamps
3. Nonces

4.11
MN-HA-Key AVP

The MN-HA-Key AVP (AVP Code TBD) is of type OctetString and contains the Key for the associated MN-HA MSA. AAAH generates the key according to [7].

4.12
MN-HA-MSA-Lifetime AVP

The MN-MSA-Lifetime AVP (AVP Code TBD) is of type Unsigned32 and represents the period of time (in seconds) for which the key or nonce of MN-HA MSA is valid.

5.
IANA Considerations

This document defines new command code and new AVP codes.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diameter Application-ID</td>
<td>TBD</td>
<td>3</td>
</tr>
<tr>
<td>MIPv6-Home-Agent-Query</td>
<td>TBD</td>
<td>3.2</td>
</tr>
<tr>
<td>MIPv6-Home-Agent-Information</td>
<td>TBD</td>
<td>3.3</td>
</tr>
<tr>
<td>MIP-binding-update AVP</td>
<td>TBD</td>
<td>4.1</td>
</tr>
<tr>
<td>MN-AAA Authenticator info AVP</td>
<td>TBD</td>
<td>4.2</td>
</tr>
<tr>
<td>MN-AAA Authenticator HMAC AVP</td>
<td>TBD</td>
<td>4.3</td>
</tr>
<tr>
<td>MN-AAA-SPI AVP</td>
<td>TBD</td>
<td>4.4</td>
</tr>
<tr>
<td>HoA AVP</td>
<td>TBD</td>
<td>4.5</td>
</tr>
<tr>
<td>CoA AVP</td>
<td>TBD</td>
<td>4.6</td>
</tr>
<tr>
<td>MIP-MN-to-HA-MSA AVP</td>
<td>TBD</td>
<td>4.7</td>
</tr>
<tr>
<td>MN-HA-Nonce AVP</td>
<td>TBD</td>
<td>4.8</td>
</tr>
<tr>
<td>MN-HA-SPI AVP</td>
<td>TBD</td>
<td>4.9</td>
</tr>
<tr>
<td>MN-Replay-Mode AVP</td>
<td>TBD</td>
<td>4.10</td>
</tr>
<tr>
<td>MN-HA-Key AVP</td>
<td>TBD</td>
<td>4.11</td>
</tr>
<tr>
<td>MN-HA-MSA-Lifetime AVP</td>
<td>TBD</td>
<td>4.12</td>
</tr>
</tbody>
</table>

6.
Security Considerations

In this document we assume that the message transfer between the HA and AAAH is secure. This could be achieved by IPsec or equivalent protocol.
References


Acknowledgments

Significant contributions to this draft were made by Vishnu Ram, Saumya Upadhyaya, Nitin Jain, Nikhil Suares, K. shivanand, Satendra G and Liyaqatali G Nadaf.

Author’s Addresses

Vihang Kamble
Motorola

Vishnu et. al Expires April 2007

[Page 9]
Full 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.

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.

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.