H. Tschofenig
T. Tsenov
Siemens
G. Giaretta
TILab
J. Bournelle
GET/INT

October 23, 2005

Mobile IPv6 Bootstrapping using Diameter
draft-tschofenig-mip6-aaa-ha-diameter-01.txt

Status of this Memo

Copyright Notice

Abstract

Both Mobile IPv6 bootstrapping solutions require use of a AAA interface. In the split scenario, this interface is between the Home Agent and the AAA infrastructure of the Mobile Service Provider (MSP) and the Mobility Service Authorizer (MSA). The first interface

should meet a list of requirements. This document provides an overview of the capabilities and design of the Diameter protocol that could meet the specified goals. In the integrated scenario, in addition to this interface, the impact of the MIPv6 bootstrapping on the AAA interface for network access authentication must be considered. Basically, this interface is also used to carry Home Agent information. This document defines the necessary AVP and how Diameter can be used in the integrated scenario.

Table of Contents

1. Introduction

In Mobile IPv6 deployment, authentication, authorization and accounting issues in the protocol operations are approached by using the AAA infrastructure. The [8] document presents a number of bootstrapping scenarios using the HA-AAA interface and defines a list of requirements that this interface should cover. In the first part, this document deals with the functional capabilities of the Diameter protocol as a AAA protocol applicable at the discussed interface.

Currently, two Mobile IPv6 bootstrapping solutions exist depending on the considered scenario. In the split scenario, only a HA-AAA interface is considered whereas in the integrated scenario both NAS-AAA and HA-AAA interface need to be addressed. This document explains how to use Diameter and its EAP and NASREQ applications to handle the AAA part of the both Mobile IPv6 bootstrapping solutions.

2. Motivation

Designed to cover network access requirements for AAA protocols [1], Diameter protocol provides a framework for applications offering AAA services. This design approach gives to the protocol extensibility, interoperability and flexibility in offering AAA solutions in comparison to other AAA protocols. Support of definition of new application Ids, commands and AVPs provides extensibility. Recommended re-use of commands and AVPs and careful consideration of the level of AVP's support provides interoperability. Usage of IPsec and TLS for transport hop-by-hop security, possible support for AVP integrity and confidentiality and usage of peer-to-peer model (any Diameter node can initiate a request message) provide flexibility of the Diameter AAA applications to fit to specific requirements.

In the following sections we try to specify by which means a possible Diameter application would cover the requirements for the HA-AAA interface specified in [8].

3. Goals

In presentation of the analysis of goals and possible design solutions by Diameter we follow the classification, labels and naming assigned in the document [8], where these goals are identified. Since several of the issues MIGHT be addressed in similar way or by similar Diameter functionality, we have grouped these issues and have given a general description of the groups.

3.1. General goals

3.1.1. G1.1 - G1.4 Security

As design goals for an AAA interface, G1.1 - G1.4 goals specify standard requirements for a AAA protocol - mutual authentication of the peers, integrity, replay protection and confidentiality. IPsec or TLS provide the hop-by-hop security. Combined, they SHOULD be able to provide the range of security services required for the HA-AAA interface.

3.1.2. Dead peer detection - the HA-AAA interface SHOULD support inactive peer detection.

Two possible approaches MIGHT be considered here:

- o AAAH server and Home Agent establish a transport connection between each other. In this case Diameter heartbeat messages called Watch-Dog-Request/Answer, which are exchanged over this connection to test for its aliveness, MAY be used to detect inactivity in any of the two Diameter peers.

- o AAAH server and Home Agent do not have transport connection. In this case inactive peer detection functionality SHOULD be provided into the Diameter session - service stateless Diameter sessions MIGHT be established between the AAAH server and the range of MSP's Home Agents for detecting HAs availability.

3.2. Service Authorization

3.2.1. G2.1. The HA-AAA interface SHOULD allow the use of Network Access Identifier (NAI) to identify the mobile node.

Identification by User-Name AVP [1], which has a format consistent with the NAI specifications, is common for Diameter applications. Diameter provides functionality for routing of Diameter requests based on the information included in the User-Name AVP.

3.2.2. G2.2. The HA SHOULD be able to query the AAAH server to verify Mobile IPv6 service authorization for the mobile node.

Based on the peer-to-peer model, Diameter design gives the functionality that any Diameter node can initiate a request message. This, combined with the support of EAP, would provide flexible solutions for this issue. Currently several Diameter application standardized or under work-in-progress address different types of authorization - network access [2], credit control [9], quality of service [10]. This MIGHT allow re-use of present AVPs over the AAAH-HA interface.

3.2.3. G2.3. The AAAH server SHOULD be able to enforce explicit operational limitations and authorization restrictions on the HA.(e.g. packet filters, QoS parameters).

Several present Diameter applications, standardized or under work-in-progress address an operation and authorization control over specific services and have defined appropriate AVPs. NAS-Filter-Rule AVP, defined by Diameter NASREQ application [2], provides IP packet filter description. QoS-Filter-Rule AVP defined by Diameter NASREQ application and QSPEC AVP defined by Diameter QoS Authorization [10] provide QoS parameter description. Credit Control application [9] provides cost control over requested services. AVPs MAY be re-used for providing required functionality over the AAAH-HA interface. This, combined with the possibility that any node can initiate request message, gives control to the AAAH server over HA's functionality.

3.2.4. G2.4 - G2.6. Issues addressing the maintenance of a Mobile IPv6 session by the AAAH server, e.g. authorization lifetime, extension of the authorization lifetime and explicit session termination by the AAAH server side.

Diameter base protocol provides a powerful set of commands and AVPs for management of the authorization and accounting sessions. A number of AVPs (Auth-Lifetime-AVP, Grace-Period-AVP, Session-Timeout-AVP) handle the duration (in time) of an authorization session [1]. Additional AVPs for measuring the authorization duration in units different that time are specified too [9]. Exchanging of application specific authorization request/answer messages provides extension of the authorization session. Initiation of the re-authorization by both sides could be supported. Both sides could initiate session termination, by using Diameter Session Termination and Abort Session messages.

All these are applied to the Diameter session used for authorization of a Mobile IPv6 session and need to be applied appropriately to this

Mobile IPv6 session too.

3.2.5. G2.7. The AAAH server SHOULD be able to retrieve the Mobile IPv6 state associated to a specific MN from the correspondent HA.

This MAY be useful to periodically verify the Mobile IPv6 service status.

This issue has two sides:

1. How the AAAH SHOULD know which HA to contact to retrieve current status of MN's Mobile IPv6 service in case of stateless MSP architecture and several servicing AAA servers? - As analyzed into the [11], this need would be required for re-authorization and in this case the provision of HA info could be provided from the MN during the re-authentication session between NM and AAAH server.

2. Once having the HA info, AAAH SHOULD contact it to verify the status of MN's Mobile IPv6 service. - This could be performed by Request/Response messages initiated by the AAAH server. This functionality is supported by the Diameter protocol and currently is applied into Diameter SIP application for updating user profiles at Diameter client (i.e., SIP server).

3.3. Accounting - G3.1. The HA-AAA interface MUST support the transfer of accounting records needed for service control and charging

Diameter accounting protocol provides a variety of options - real-time accounting, event/session-type accounting records, fault resilience, correlation of accounting records. Requirements for the accounting services over AAAH-HA interface are standard. Definition or re-used of AVPs for the specific accounting records combined with the functionality of the Diameter accounting protocol SHOULD provide desired accounting services.

3.4. Mobile Node Authentication (G4.1. and G4.2.)

These issues require the functionality of AAAH server working as a back-end authentication server and HA working as NAS and EAP authenticator in pass-through mode for providing a mobile node authentication. These functionalities are provided by Diameter NASREQ and EAP applications, and MIGHT be re-used at the AAAH-AH interface.[2], [3]

3.5. Provisioning of configuration parameters

Issues G5.1 - G5.3 are related to capability of exchanging and negotiating of operational parameters for Mobile IPv6 protocol bootstrapping and providing appropriate security level for this information.

Diameter provides secure transport by means of IPsec, TLS and possible AVPs integrity and confidentiality support (currently with no interest from the community). Several AVPs could be re-used for carrying the operational parameters for the Mobile IPv6 bootstrapping. Framed-IPv6-Prefix AVP, Login-IPv6-Host AVP, Framed-Interface-Id AVP, Framed-IPv6-Route AVP defined by NASREQ MIGHT be used for home address provision and AVPs defined in EAP application MIGHT be used for key transport [3].

4. Bootstrapping Mobile IPv6 in the split scenario

In the split scenario for bootstrapping Mobile IPv6 [4], the MN discovers HA through DNS mechanism. Then it uses IKEv2 [5] to setup IPsec SAs. IKEv2 supports EAP to authenticate the Initiator and thus the MN. As such, the MN can use its credentials (obtained from the MSA) to be authenticated for the IPv6 mobility service. The HA MAY rely on a EAP server co-located on a AAA server for this purpose. In this case, a HA-AAA interface is needed. This interface MUST support transport of EAP packets.

```
+----+      IKEv2  +----+    Diameter EAP      +---+
| MN |<----------->| HA |<-------------------->|AAA|
+----+             +----+                      +---+
```

Figure 1: Diameter EAP as the HA-AAA interface in Split scenario

For this purpose, the HA can use Diameter EAP Application [3] (cf. Figure 1). As shown in the previous section, this protocol fulfill goals described in [8]

```
   MN                             HA                       AAAH
   --                             --                       ----
            IKE_SA_INIT
   <------------------------------>

    HDR, SK{IDi,[CERTREQ,] [IDr,]
            SAi2, TSi, TSr}
   ------------------------------->
                                       DER (EAP-Response)
                                    ------------------------->
                                       DEA (EAP-Request)
                                    <-------------------------
    HDR, SK {IDr, [CERT,] AUTH,
             EAP }
   <-------------------------------
    HDR, SK {EAP}
   -------------------------------->
                                       DER (EAP-Response)
                                    ------------------------->
                                       DEA (EAP-Request)
                                    <-------------------------
    HDR, SK{EAP-Request}
   <-------------------------------
    HDR, SK{EAP-Response}
   -------------------------------->
                                       DER (EAP-Response)
                                    ------------------------->
             ...                             ...

                                       DEA (EAP-Success)
                                    <-------------------------
    HDR, SK{EAP-Success}
   <-------------------------------
    HDR, SK{AUTH}
   ------------------------------->
    HDR, SK {AUTH, SAr2, TSi, TSr }
   <-------------------------------
```

Figure 2: IKEv2 Diameter EAP

MN and HA start with an IKE_SA_INIT to setup the IKE SA. The MN indicates its desire to use EAP by not including the AUTH payload in the third message. However it indicates its identity (e.g. NAI) by using the IDi field. If the HA supports EAP for authentication, it forwards the identity to the AAAH by sending a Diameter-EAP-Request (DER) message containing the identity in the EAP-Payload AVP and in the User-Name AVP. Based on this identity, the AAAH chooses an

authentication method and sends the first EAP-Request in the Diameter-EAP-Answer message. During the EAP authentication phase, the HA relays EAP packets between the MN and the AAAH. If the authentication succeeds and if the MN is authorized to use Mobile IPv6 service, the AAAH sends a DEA message containing the EAP-success and the AAA-Key derived from the EAP authentication method . Note that EAP authentication methods that do not derive keys are not recommended. This key is used by both MN and HA to generate the AUTH payload. In the latter message, MN and HA finish to setup IPsec SAs for Mobile IPv6.

5. Bootstrapping Mobile IPv6 in the integrated scenario based on DHCP

The Figure 3 represents the components and architecture of the Mobile IPv6 bootstrapping solution in the integrated scenario. This figure is extracted from [6].

```
                                         |
                     ASP(/MSP)           |   ASA/MSA(/MSP)
                                         |
                                         |
                     +-------+           |        +-----+
                     | AAAL  |-----------|--------|AAAH |
                     +-------+           |        +-----+
                         |               |
                         |               |
                         |               |
                         |               |
                         |               |
                     +-----+    +------+ |
         +----+      |     |    |DHCP  | |
         | MN |------| NAS/|----|Server| |
         +----+      |Relay|    |      | |
                     +-----+    +------+ |
                                         |
                                         |
                     +--------+          |      +--------+
                     | HA     |          |      | HA     |
                     | in ASP |          |      |in MSP  |
                     +--------+          |      +--------+
```

Figure 3: Mobile IPv6 Bootstrapping: Integrated scenario

In the solution for the Integrated scenario based on DHCP [6], the HA is allocated during the network access authentication phase. Then, the MN queries a HA by using DHCPv6 (the NAS acting as a DCHPv6 relay). In this scenario, it is the same entity that authorizes Network Access (ASA) and Mobility Service (MSA). The current solution [6] allows the MN to require a local HA (in the visited ASP) by specifying it in its DHCPv6 request. Even in this case, the AAAH allocates a HA from the home MSP. The Home Agent information is sent during the AAA exchange for network access authentication. After this, the MN initiates an IKEv2 exchange with the allocated HA as described in the previous section.

Diameter EAP [3] or NASREQ [2] applications are used as Diameter AAA protocols for network access. As we are combining network access and

mobility authorization, the Home Agent information SHOULD be sent when the MN is correctly authenticated. For this reason, the AVP containing HA information MUST be sent in a AAA message containing the success authentication. For Diameter EAP, this AVP will be carried in a DEA message containing the EAP-Payload AVP with EAP-Success. For Diameter-NASREQ, the AVP MUST be carried in AA-Answer containing the Result-Code AVP indicating a success.

5.1. Home-Agent AVP

The Home-Agent AVP (AVP Code To Be Assigned) is of type OctetString and contains the IPv6 address of the allocated Home Agent. The 'M" bit in the header of the Home-Agent AVP MUST be cleared, otherwise if the NAS does not support it, the authentication will fail.

6. Conclusion

This document provides information about the Diameter usage for both split and integrated scenarios for Mobile IPv6 bootstrapping. It is not yet complete since the goals for the HA-AAA interface [8] are still work in progress.

7. Security considerations

[Editor's Note: Since the document is not complete it is necessary to state that the security consideration section is incomplete as well. Hence, it is only possible to refer to the security issues raised in the Mobile IPv6 and Diameter protocol related documents mentioned here, such as [11], [8] and [1].]

8. IANA Considerations

The AVP code for the Home-Agent AVP needs to be allocated.

9. Acknowledgements

We would like to thank the MIPv6 Bootstrapping Design Team for their comments. Additionally, we would like to thank Junghoon Jee for his feedback.

10. References

10.1. Normative References

[1] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[2] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", RFC 4005, August 2005.

[3] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", RFC 4072, August 2005.

[4] Giaretta, G., "Mobile IPv6 bootstrapping in split scenario", draft-ietf-mip6-bootstrapping-split-01 (work in progress), October 2005.

[5] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-17 (work in progress), October 2004.

[6] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping via DHCPv6 for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-00 (work in progress), October 2005.

[7] Hamilton, M. and R. Wright, "Use of DNS Aliases for Network Services", BCP 17, RFC 2219, October 1997.

10.2. Informative References

[8] Giaretta, G., "Goals for AAA-HA interface", draft-ietf-mip6-aaa-ha-goals-00 (work in progress), May 2005.

[9] Mattila, L., Koskinen, J., Stura, M., Loughney, J., and H. Hakala, "Diameter Credit-control Application", draft-ietf-aaa-diameter-cc-06 (work in progress), August 2004.

[10] Alfano, F., "Diameter Quality of Service Application", draft-alfano-aaa-qosprot-04 (work in progress), September 2005.

[11] Giaretta, G., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), October 2004.

Authors' Addresses

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

Email: Hannes.Tschofenig@siemens.com

Tseno Tsenov
Siemens
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

Email: tseno.tsenov@mytum.de

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO,   10148
Italy

Email: gerardo.giaretta@tilab.com

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France

Email: julien.bournelle@int-evry.fr

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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