Mobility for IPv6 (mip6)
Internet-Draft
Expires: January 12, 2006

H. Tschofenig
T. Tsenov
Siemens
G. Giaretta
TILab
J. Bournelle
GET/INT
July 11, 2005

Diameter applicability for AAA-HA Interface in Mobile IPv6
draft-tschofenig-mip6-aaa-ha-diameter-00.txt

Status of this Memo

Copyright Notice

Abstract

In Mobile IPv6 deployment a need for interface between the Home Agent and the AAA infrastructure of the Mobile Service Provider (MSP) and the Mobility Service Authorizer (MSA) has been identified. This interface should meet a list of requirements. This document provides

an overview description of the functionalities and design of Diameter protocol which could meet the specified goals.

Table of Contents

1. Introduction

In Mobile IPv6 deployment, authentication, authorization and accounting issues in the protocol operations are approached by definition of an interface between the Home Agent (HA) and the AAA infrastructure of the Mobility Service Provider (MSP). [3] document presents a number of bootstrapping scenarios using the AAA-HA interface and defines a list of requirements that the interface should cover. This document deals with the functionalities provided by Diameter protocol as a AAA protocol applicable at the discussed interface.

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 AAA-HA interface specified in [3].

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 [3], 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. Various authentication methods might be used, many of them are already supported by a Diameter NASREQ and EAP applications [4],[5] and could be re-used. IPsec or TLS provide the hop-by-hop security. Combined, they should be able to provide the range of security services required for the AAA-HA interface.

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

Two possible approaches might be considered here:

- 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.

- 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 AAA-HA 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 [4], credit control [6], quality of service [7]. 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 [4], provides IP packet filter description. QoS-Filter-Rule AVP defined by Diameter NASREQ application and QSPEC AVP defined by Diameter QoS Authorization [7] provide QoS parameter description. Credit Control application [6] 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 [6]. 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 [8], 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 AAA-HA 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.[4], [5]

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 [5].

4. Conclusion

This document provides information about the Diameter usage for the AAA-HA interface. It is not yet complete since (a) the goals for the AAA-HA interface [3] are still work in progress and (b) solutions for all scenarios are not yet available. A final conclusion about the required AVPs cannot be provided at this point in time.

5. 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 [8], [3] and [1].]

6. IANA Considerations

This document does not require actions to be taken by the IANA.

7. Acknowledgements

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

8. References

8.1 Normative References

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

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

8.2 Informative References

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

[4] Calhoun, P., Zorn, G., Spence, D., and D. Mitton, "Diameter Network Access Server Application", draft-ietf-aaa-diameter-nasreq-17 (work in progress), July 2004.

[5] Eronen, P., Hiller, T., and G. Zorn, "Diameter Extensible Authentication Protocol (EAP) Application", draft-ietf-aaa-eap-10 (work in progress), November 2004.

[6] 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.

[7] Alfano, F., "Diameter Quality of Service Application", draft-alfano-aaa-qosprot-02 (work in progress), February 2005.

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

[9] Garcia-Martin, M., "Diameter Session Initiation Protocol (SIP) Application", draft-ietf-aaa-diameter-sip-app-07 (work in progress), March 2005.

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

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

Copyright Statement

Acknowledgment

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