MIP6 Working Group
Internet Draft
Expires: March 2005

G. Giaretta
I. Guardini
E. Demaria
TILab
J. Bournelle
GET/INT
R. Lopez
Univ. of Murcia
September 2004

Goals for AAA-HA interface
<draft-giaretta-mip6-aaa-ha-goals-00.txt>

Status of this Memo

Abstract

In commercial deployments Mobile IPv6 can be a service offered by a Mobility Services Provider (MSP). In this case all protocol operations may need to be explicitely authorized and traced. A convenient approach to do that is to define an interface between the Home Agent (HA) and the AAA infrastructure of the MSP, which stores user's credentials and service profiles. The availability of this interface can be useful also to enable dynamic Mobile IPv6 bootstrapping on both the mobile node and the designated HA. This document describes various scenarios where an interface between the HA and the AAA infrastructure of the MSP is required. Furthermore, a list of design goals for this interface is provided.

Table of Contents

1. Introduction

Mobile IPv6 [1] was originally designed as a standalone protocol to handle terminal mobility relying on a centralized and pre-configured Home Agent (HA). Nonetheless, if Mobile IPv6 is a service offered by a Mobility Services Provider (MSP), all protocol operations may need to be explicitely authorized and traced (e.g. for accounting purposes). A convenient approach to achieve this result is to define an interface between the AAA infrastructure of the MSP and the HA. Such an interface may be useful also in some Mobile IPv6 dynamic bootstrapping scenarios [2].

This document describes various scenarios for which an interface between the HA and the AAA infrastructure of the MSP is useful. Furthermore, a list of goals for such an interface is provided.

No assumptions are made on the protocol used to implement the interface. An obvious choice may be the employment of a AAA protocol such as RADIUS or Diameter. Nonetheless, for some scenarios, other non AAA protocols such as SNMPv3 [4] or COPS-PR [5] may satisfy all the goals described herewith.

2. Motivation

Mobile IPv6 specification [1] requires that Mobile Nodes (MNs) are provisioned with a set of configuration parameters, namely the Home Address and the Home Agent Address, in order to accomplish a home registration. Moreover MNs and Home Agents (HAs) must share the cryptographic material needed to protect Mobile IPv6 signaling (e.g. shared keys or certificates to setup an IPsec security association).

The simplest option is to statically provision all the necessary configuration data on MNs and HAs. This solution raises obvious scalability issues especially in a large network with a lot of users (e.g. a mobile operator network). For this reason the dynamic Mobile IPv6 bootstrapping problem is currently under study [2].

In case Mobile IPv6 is a service offered by a Mobility Service Provider (MSP) all protocol operations (e.g. home registrations) may need to be explicitely authorized and monitored (e.g. for accounting purposes). This can be done relying on the AAA infrastructure of the MSP, that stores users' service profiles and credentials.

The deployment of this service model requires the availability of an interface between the AAA infrastructure and the HA, that can be seen as the Network Access Server (NAS) for Mobile IPv6. The core capabilities that should be supported by this interface include Mobile IPv6 service authorization and maintenance (e.g. asynchronous service termination) as well as the exchange of accounting data. This is the basic set of features needed in any Mobile IPv6 bootstrapping scenario (i.e. static or dynamic).

Moreover, whenever static provisioning is not feasible, the AAA infrastructure of the MSP can be used as the central element to build a dynamic Mobile IPv6 bootstrapping solution. In this case the AAA infrastructure can be exploited also to send to the designated HA the needed configuration parameters (e.g. keying material) as well as to assist the HA with mobile node authentication.

There is therefore space for the definition of a general AAA-HA communication interface capable to support the basic features described above (e.g. authorization and accounting) as well as the extended capabilities (e.g. transfer of configuration data) needed to enable various dynamic Mobile IPv6 bootstrapping scenarios.

3. Basic security model

The basic security model behind this draft assumes that the mobile node shares a pre-configured trust relationship with the AAA server of the MSP (AAAH), as stated in [2]. Furthermore the HA is expected to share a trust relationship with the AAAH server (see Figure 1).

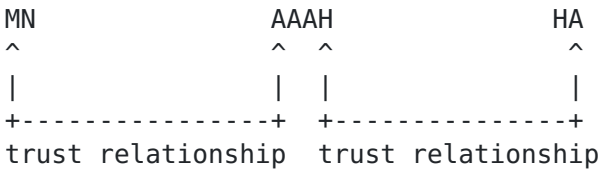

Figure 1 - Basic Model

4. Bootstrapping scenarios

This section describes some bootstrapping scenarios in which a communication between the AAA infrastructure of the Mobility Service Provider and the Home Agent is needed. These scenarios include both dynamic (Scenario 1 and Scenario 2) and static (Scenario 3 and Scenario 4) bootstrapping.

4.1 Scenario 1

In this scenario, depicted in Figure 2, the MN discovers the Home Agent address (e.g. by means of a new DNS SRV record or DHCP) and performs an IKEv2 [3] exchange with the HA to setup the IPsec SA needed to protect mobility signaling. Eventually, during this handshake, the MN can also obtain a valid Home Address from the HA.

The MN is not expected to share a pre-configured trust relationship with the HA, nor to share a secret with it. For this reason, peer authentication in IKEv2 can be performed through an EAP exchange. The HA, behaving as an EAP authenticator operating in pass-through mode, forwards this EAP exchange to the AAAH server, that can authenticate the MN and authorize the Mobile IPv6 service. Therefore, in this case an interface between the HA and the AAAH server is needed at least for authentication and authorization purposes.

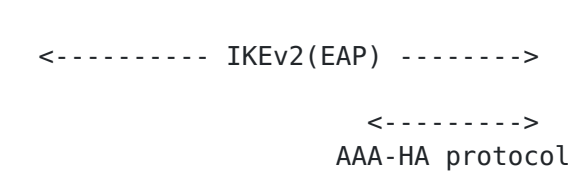

Figure 2 - Dynamic MIPv6 bootstrapping through IKEv2 and EAP

4.2 Scenario 2

In this scenario Mobile IPv6 bootstrapping is performed during network access authentication (it is assumed that the access provider and the MSP are the same entity, i.e. Integrated ASP [2]) and the AAA server of the MSP (AAAH) controls the whole bootstrapping procedure interacting with both the mobile node and the designated HA.

The AAAH server and the MN can exploit AAA routing to exchange configuration data. Possible approaches to implement this communication are the following:

- if network access authentication is carried out using EAP, it is possible to piggyback Mobile IPv6 configuration parameters (e.g.

Home Agent address, Home Address) within the EAP exchange [6]. See Figure 3;

- alternatively, Mobile IPv6 parameters can be transferred to the Network Access Server (NAS) by means of RADIUS or Diameter AVPs [7] and then forwarded to the MN through other means (e.g. L2-specific extensions, DHCP [8]). See Figure 4 for an example.

In both cases, the AAAH server must communicate with the designated HA to select a suitable Home Address for the MN and to deliver to the HA the necessary configuration parameters (e.g. pre-shared key for IKE bootstrapping). Therefore also in this scenario an interface between the AAAH server and the HA must be defined for parameter exchange as well as authentication and Mobile IPv6 service authorization.

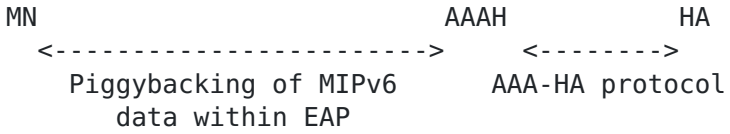

Figure 3 - MIPv6 bootstrapping with piggybacking within EAP

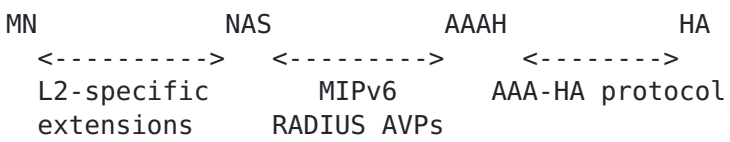

Figure 4 - MIPv6 bootstrapping with RADIUS AVPs

4.3 Scenario 3

In this scenario the MN is statically provisioned with the data needed to bootstrap Mobile IPv6 service (i.e. Home Agent Address, Home Address and a shared secret with the HA). For example, the MN can be configured with a pre-shared key to dynamically establish an IPsec Security Association with the HA using IKE.

However, in general the static configuration of these parameters and the authentication performed through the pre-shared key may not be sufficient to conclude that the MN is authorized for MIPv6 service. For example, the MSP might want to prevent the usage of MIPv6 if the the credit of the MN is going to exhaust. Moreover, there might be the need for the MSP to enforce more complex dynamic authorization policies based on time of day and/or visited location.

This implies that during the IKE exchange the HA must communicate with the AAAH server in order to explicitly authorize MIPv6 service for that particular MN. See Figure 5.

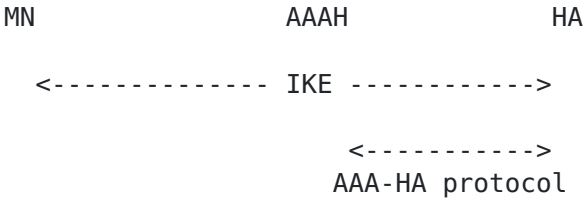

Figure 5 - Mobile IPv6 authorization with static boostrapping

4.4 Scenario 4

In this scenario, the IPsec SA between MN and HA is statically and manually configured, thus the MN does not need to perform an IKE exchange with the HA. The MN activates MIPv6 service, sending a Binding Update message to the HA in order to update its location.

The presence of the IPsec SA between MN and HA is enough in order to authenticate the binding management messages. However, it is not enough to authorize MIPv6 service; thus, as soon as it receives a Binding Update, the HA must explicitly authorize MIPv6 service interacting with the AAAH server (Figure 6). For this purpose, an interface between the HA and the AAAH is needed at least for authorization purposes.

If deemed necessary, the explicit authorization of Binding Updates based on the handshake depicted in Figure 5 can be used also in the bootstrapping scenarios described in the previous sections. It may be useful to enforce dynamic authorization policies, such as those based on the MN's location.

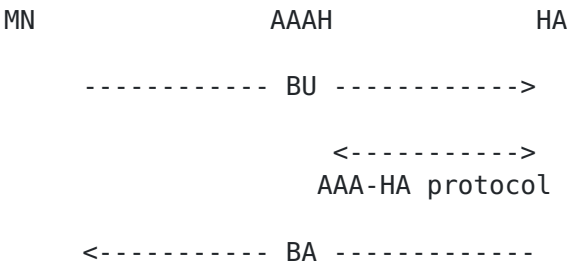

Figure 6 - Binding Update Authorization

5. Goals for the AAA-HA interface

The motivations and scenarios illustrated in previous sections raise the need to define an interface between the AAAH server and the HA. The following sections list a set of goals for this interface.

5.1 General goals

G1.1 The AAAH server and the HA must be able to authenticate each other (mutual authentication) in order to prevent the installation of unauthorized state on the HA.

G1.2 The AAA-HA interface must provide integrity protection in order to prevent any alteration of exchanged data (e.g. Mobile IPv6 configuration parameters).

G1.3 The AAA-HA interface must provide replay protection.

G1.4 The AAA-HA interface should provide confidentiality since it may be used to transfer security parameters (e.g. IKE pre-shared key).

G1.5 The AAA-HA interface should support inactive peer detection. This functionality can be used by the AAAH server to maintain a list of active HAs (e.g. useful for HA selection).

5.2 Service Authorization

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

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

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).

G2.4 The AAAH server should be able to send an authorization lifetime to the HA to limit Mobile IPv6 session duration for the MN.

G2.5 The HA should be able to request to the AAAH server an extension of the authorization lifetime granted to the MN.

G2.6 The AAAH server should be able to force the HA to terminate an active Mobile IPv6 session for authorization policy reasons (e.g. credit exhaustion).

G2.7 The AAAH server should be able to retreive 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.

5.3 Accounting

G3.1 The AAA-HA interface must support the transfer of accounting records needed for service control and charging. These include (but may not be limited to): time of binding cache entry creation and deletion, octets sent and received by the mobile node in Bi-directional Tunneling, etc.

5.4 Mobile Node Authentication

G4.1 The AAA-HA interface should support MN authentication (and re-authentication) with the HA working as a NAS and the AAAH server working a back-end authentication server.

G4.2 The AAA-HA interface should support at least pass-through EAP authentication with the HA working as a EAP authenticator operating in pass-through mode and the AAAH server working as back-end authentication server.

5.5 Provisioning of configuration parameters

G5.1 The AAAH server should be able to poll the designated HA for the allocation of a Home Address to the MN. Optionally, the AAAH server can provide a set of hints for the construction of the Home Address (e.g. a preferred Home Address or a preferred Interface Identifier).

G5.2 The HA should be able to communicate to the AAAH server the Home Address allocated to the MN.

G5.3 The AAAH server should be able to send to the HA the security data needed to setup the IPsec SA between the MN and the HA. Possible security data are the authentication method and the cryptographic material to be used for IKE bootstrapping.

6. Mapping between goals and scenarios

The table below shows which goals, among those listed in section 5, are strictly (X) or optionally (O) required for each of the scenarios discussed in section 4.

Section Defined	Goals	Scen. 1	Scen. 2	Scen. 3	Scen. 4
5.1	G1.1	X	X	X	X
	G1.2	X	X	X	X
	G1.3	X	X	X	X
	G1.4	O	X	O	O
	G1.5	X	X	X	X
5.2	G2.1	X	X	O	O
	G2.2	X	X	X	X
	G2.3	X	X	X	X
	G2.4	X	X	X	X
	G2.5	X	X	X	X
	G2.6	X	X	X	X
	G2.7	X	X	X	X
5.3	G3.1	X	X	X	X
5.4	G4.1	X			
	G4.2	X			
5.5	G5.1		X		
	G5.2		X		
	G5.3		X		

7. Security Considerations

As stated in section 5.1 the AAA-HA interface must provide mutual authentication, integrity and replay protection. Furthermore, if security paramters (e.g. IKE pre-shared key) are transferred through this interface, confidentiality support is also required.

References

[1] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24 (work in progress), July 2003.

[2] Patel, A. et al. "Problem Statement for bootstrapping Mobile IPv6", draft-ietf-mip6-bootstrap-ps-00 (work in progress), July 2004.

[3] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-16 (work in progress), September 2004.

[4] Case, J., Mundy, R., Partain, D. and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

[5] K. Chan, D. Durham, S. Gai, S. Herzog, K. McCloghrie, F. Reichmeyer, J. Seligson, A. Smith, R. Yavatkar, "COPS Usage for Policy Provisioning,", RFC 3084, March 2001.

[6] Giaretta, G., Guardini, I., Demaria, E., Bournelle, J., Laurent-Maknavicius, M., "MIPv6 Authorization and Configuration based on EAP", draft-giaretta-mip6-authorization-eap-02 (work in progress), September 2004.

[7] Chowdhury, K. and Lior, A., "RADIUS Attributes for Mobile IPv6 bootstrapping", draft-chowdhury-mip6-bootstrap-radius-00 (work in progress), July 2004.

[8] Jang, H. J. and Yegin, A., "DHCP Option for Home Agent Discovery in MIPv6", draft-jang-dhc-haopt-00 (work in progress), May 2004.

Authors' Addresses

Gerardo Giaretta
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2286904
Email: gerardo.giaretta@tilab.com

Ivano Guardini
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2285424
Email: ivano.guardini@tilab.com

Elena Demaria
Telecom Italia Lab
via G. Reiss Romoli, 274
10148 TORINO
Italy
Phone: +39 011 2285403
Email: elena.demaria@tilab.com

Julien Bournelle
GET/INT
9 rue Charles Fourier
Evry 91011
France
Email: julien.bournelle@int-evry.fr

Rafa Marin Lopez
University of Murcia
30071 Murcia
Spain
EMail: rafa@dif.um.es

Intellectual Property Statement

Full Copyright Statement

Disclaimer of Validity

Acknowledgment

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