MEXT Working Group
Internet-Draft
Expires: June 29, 2008

G. Giaretta
Qualcomm
I. Guardini
E. Demaria
Telecom Italia
J. Bournelle
Orange Labs
R. Lopez
Univ. of Murcia
December 27, 2007

AAA Goals for Mobile IPv6
draft-ietf-mext-aaa-ha-goals-00

Status of this Memo

Copyright Notice

Abstract

In commercial and enterprise deployments Mobile IPv6 can be a service offered by a Mobility Services Provider (MSP). In this case all

protocol operations may need to be explicitly authorized and traced, requiring the interaction between Mobile IPv6 and the AAA infrastructure. Integrating the AAA infrastructure (e.g. NAS and AAA server) offers also a solution component for Mobile IPv6 bootstrapping. This document describes various scenarios where a AAA interface for Mobile IPv6 is required. Additionally, it lists design goals and requirements for such an interface.

Table of Contents

1. Introduction

Mobile IPv6 [1] provides the basic IP mobility functionality for IPv6. When Mobile IPv6 is used in tightly managed environments with the use of the AAA (Authentication, Authorization and Accounting) infrastructure, an interface between Mobile IPv6 and AAA protocols needs to be defined. Also, two scenarios for bootstrapping Mobile IPv6 service [2] , i.e., split [3] and integrated [4] scenarios, require the specification of a message exchange between the HA and AAA infrastructure for authentication and authorization purposes and a message exchange between the AAA server and the NAS in order to provide the visited network with the necessary configuration information (e.g. Home Agent address).

This document describes various scenarios where a AAA interface is required. Additionally, it lists design goals and requirements for the communication between the HA and the AAA server and the NAS and the AAA server needed in the split and integrated scenarios. Requirements are listed in case either IPsec or rfc 4285 [5] is used for Mobile IPv6 authentication.

This document only describes requirements, goals and scenarios. It does not provide solutions.

Notice that this document builds on the security model of the AAA infrastructure. As such, the end host/user shares credentials with the home AAA server and the communication between the AAA server and the AAA client may be protected. If the AAA server and the AAA client are not part of the same administrative domain, then some sort of contractual relationship between the involved administrative domains is typically in place in form of roaming agreements.

2. Terminology

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 [6], with the qualification that unless otherwise stated these words apply to the design of the AAA protocol extension, not its implementation or its usage.

Some of the terms are also extracted from [2].

- Access Service Authorizer (ASA). A network operator that authenticates a mobile node and establishes the mobile node's authorization to receive Internet service.

- o Access Service Provider (ASP). A network operator that provides direct IP packet forwarding to and from the end host.
- o Mobility Service Authorizer (MSA). A service provider that authorizes Mobile IPv6 service.
- o Mobility Service Provider (MSP). A service provider that provides Mobile IPv6 service. In order to obtain such service, the mobile node must be authenticated and prove authorization to obtain the service.

3. 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 in order to setup IPsec security associations to protect Mobile IPv6 signaling (e.g. shared keys or certificates). This is referred as the bootstrapping problem: as described in [2], the AAA infrastructure can be used as the central element to enable dynamic Mobile IPv6 bootstrapping. In this case the AAA infrastructure can be exploited to offload the end host's authentication to the AAA server as well as to deliver the necessary configuration parameters to the visited network.

Moreover, 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 explicitly authorized and monitored (e.g., for accounting purposes). This can be accomplished relying on the AAA infrastructure of the MSA that stores user profiles and credentials.

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. The need of a MIPv6-aware communication between the AAA server and the Network Access Server (NAS) is also described. For more details, please refer to the bootstrapping documents [2], [3] and [4].

4.1. Split Scenario

In the split scenario [3], there is the assumption that the mobility service and network access service are not provided by the same administrative entity. This implies that the mobility service is authorized by the MSA that is a different entity from the ASA.

In this scenario, the Mobile Node discovers the Home Agent Address using the Domain Name Service (DNS). It queries the address based on the Home Agent name or by service name. In the former case, the Mobile Node is configured with the Fully Qualified Domain Name (FDQN) of the Home Agent. In the latter case, [3] defines a new service resource record (SRV RR).

Then the Mobile Node performs an IKEv2 [8] exchange with the HA to setup IPsec SAs (to protect Mobile IPv6 signaling) and to configure its Home Address (HoA). Mutual authentication for IKEv2 between Mobile Node and Home Agent can be done with or without use of Extensible Authentication Protocol (EAP).

If EAP is used for authentication, the operator can choose any available EAP methods. Use of EAP with the AAA infrastructure allows the HA for not necessarily maintaining authentication credentials for each Mobile Node by itself. It also allows roaming in terms of Mobile IPv6 service where MSP and MSA belong to different administrative domains.

The Mobile Node may also want to update its FQDN in the DNS with the newly allocated Home Address. [3] recommends that the HA performs the DNS entry update on behalf of the Mobile Node. For that purpose, the Mobile Node indicates its FDQN in the IKEv2 exchange (IDi field in IKE_AUTH) and adds a DNS Update Option in the Binding Update message sent to the HA.

When the Mobile Node uses a Home Agent belonging to a different administrative domain (MSP != MSA), the local HA may not share a security association with the home DNS server. In this case, [3] suggests that the home AAA server is responsible for the update. Thus, the HA should send to the home AAA server the (FDQN, HoA) pair.

4.2. Integrated Scenario

In the integrated scenario [4], the assumption is that the Access Service Authorizer (ASA) is same as the Mobility Service Authorizer (MSA).

The Home Agent can the assigned either in the Access Service Provider's network or in the seprate network. In the former case, the MSP is the same entity as the ASP, whereas in the latter case MSP and ASP are different entities.

In this scenario, Mobile Node discovers the Home Agent Address using DHCPv6. If the user is authorized for Mobile IPv6 service, during the network access authentication the AAAH sends the information about the assigned home agent to the Network Access Server (NAS)

where the Mobile Node is currently attached. To request home agent data, the Mobile Node sends a DHCPv6 Information Request to the All_DHCP_Relay_Agents_and_Servers multicast address. With this request, the Mobile Node can specify if it wants a home agent provided by the visited domain (ASP/MSP) or by the home domain (ASA/MSA). In both cases, the NAS acts a DHCPv6 relay. When the NAS receives the DHCPv6 Information Request then it sends home agent information received from AAAH in a new DHC Relay Agent Option as defined in [4].

In case the Mobile Node cannot acquire home agent information via DHCPv6, it can try the default mechanism based on DNS described in [3]. After the Mobile Node has acquired the home agent information, the mechanism used to bootstrap the HoA, IPsec Security Association, and Authentication and Authorization with the MSA is the same described in the bootstrapping solution for split scenario [3].

5. Goals for AAA-HA interface

Section 4 raises the need to define extensions for the AAA protocol used between the AAA server of the MSA and the HA. The following sections list the goals for such an interface. This communication is needed for both split and integrated scenario.

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. In some deployment scenarios, it may not be feasible for HA and AAA server to mutually authenticate each other. In such a case, several AAA intermediate proxies could forward MIP6 bootstrapping information between HA and AAA. Thus, to prevent the installation of unauthorized state on the HA, the path between HA and AAAH should be secure.

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.

5.2. Service Authorization

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

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

G2.3 The AAAH server MAY assign explicit operational limitations and authorization restrictions on the HA (e.g., packet filters, QoS parameters).

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

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

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

G2.7 The HA MUST be able to indicate the IPv6 HoA that will be assigned to the MN.

G2.8 The AAAH server MUST be able to authorize the MN to use an IPv6 HoA.

G2.9 The AAAH server MUST be able to indicate to the HA whether return routability test (HoT, HoTi) shall be permitted or not via the HA for a given MN.

G2.10 The AAAH server MUST be able to authorize the MN for Dual Stack operation [9].

G2.11 The AAAH server MUST be able to indicate to the HA whether the bearer traffic for the MN needs to receive IPsec ESP protection.

G2.12 The HA MUST be able to authenticate the MN through the AAAH in case a pre-share key is used in IKEv2 for user authentication. The exact procedure is part of the solution space.

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 MUST allow the HA to act as a pass-through EAP authenticator.

G4.2 The AAA - HA interface SHOULD support authentication based on the Mobility Message Authentication Options defined in [5].

G4.3 The HA SHOULD be able to request either the keying material to generate MN-HA key for MN-HA Mobility Message Authentication Option or SHOULD be able to request the MN-HA key and the related SPI values from the AAAH server.

G4.4 The HA SHOULD be able to request the AAAH server to authenticate the MN with the value in the MN-AAA Mobility Message Authentication Option.

G4.5 The HA MUST include the Mobile Node Identifier option [7] in the AAA transactions with the AAAH server.

G4.6 The AAAH server SHOULD be able to authenticate the MN identified by the value in the Mobile Node Identifier option using the value in MN-AAA Mobility Message Authentication Option and the corresponding value of the SPI.

G4.7 If the MN-AAA Mobility Message Authentication Option is not included by the HA or the MN-AAA Mobility Message Authentication Option is included and the MN-AAA authentication is successful, the AAAH MUST send the keying material for MN-HA key to the HA if the HA requested for MN-HA keying material only. The AAAH MUST send the MN-HA key and the corresponding SPI value to the HA if the HA requested for MN-HA key and SPI.

5.5. Provisioning of Configuration Parameters

- The HA SHOULD be able to communicate to the AAAH server the Home Address allocated to the MN and the FQDN of the MN (e.g., for allowing the AAAH server to perform a DNS update on behalf of the MN).

- The AAAH SHOULD be able to indicate to the HA if the MN is authorized to autoconfigure its Home Address.

6. Goals for the AAA-NAS interface

In the integrated scenario, the AAA server provides the HA information to the NAS as part of the whole AAA operations for network access.

G6.1 The AAAH server MUST be able to communicate the Home Agent Information (IP Address or FQDN) to the NAS.

G6.2 The NAS SHOULD be able to notify the AAAH of the functionalities described in [4].

G6.3 The ASP/MSP SHOULD be able to indicate to the MSA if it can allocate a Home Agent to the MN. Therefore the NAS SHOULD be able to include suggested HA address in the ASP in the NAS - AAA interaction.

G6.4 The AAA server of the MSA MUST be able to indicate to the NAS whether the MN is authorized to use a local Home Agent (i.e. a Home Agent in the ASP/MSP).

G6.5 The overall AAA solution for integrated scenario MUST support the scenario where the AAA server of the ASA/MSA used for network access authentication is different from the AAA server used for mobility service authentication and authorization.

7. IANA Considerations

This document does not require actions by IANA.

8. Security Considerations

As stated in Section 5.1 the AAA-HA interface must provide mutual authentication, integrity and replay protection. Furthermore, if security parameters (e.g., IKE pre-shared key) are transferred through this interface, confidentiality is strongly recommended to be supported. In this case the links between the HA and the AAA server of the MSA and between the NAS and the AAA server must be secure.

9. Acknowledgements

The authors would like to thank James Kempf, Alper Yegin, Vijay Devarapalli, Basavaraj Patil, Gopal Dommety and Madjid Nakhjiri for their comments and feedback. Moreover the authors would like to thank Hannes Tschofenig for his deep technical and editorial review

of the draft. Finally the aithors would like to thank Kuntal Chowdhury who contribbuted identifying the goals related to rfc4285 authentication.

10. References

10.1. Normative References

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

[2] Patel, A. and G. Giaretta, "Problem Statement for bootstrapping Mobile IPv6 (MIPv6)", RFC 4640, September 2006.

[3] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[4] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", draft-ietf-mip6-bootstrapping-integrated-dhc-05 (work in progress), July 2007.

[5] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[6] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

10.2. Informative References

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

[9] Soliman, H., "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mip6-nemo-v4traversal-06 (work in progress), November 2007.

Authors' Addresses

Gerardo Giaretta
Qualcomm
5995 Morehouse Drive
San Diego, 92109
USA

Email: gerardog@qualcomm.com

Ivano Guardini
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Email: ivano.guardini@telecomitalia.it

Elena Demaria
Telecom Italia Lab
via G. Reiss Romoli, 274
TORINO, 10148
Italy

Email: elena.demaria@telecomitalia.it

Julien Bournelle
Orange Labs

Email: julien.bournelle@gmail.com

Rafa Marin Lopez
University of Murcia
30071 Murcia
Spain

Email: rafa@dif.um.es

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).