Network Working Group
Request for Comments: 5637
Category: Informational

G. Giaretta
Qualcomm
I. Guardini
E. Demaria
Telecom Italia
J. Bournelle
Orange Labs
R. Lopez
University of Murcia

September 2009

Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6

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 Authentication, Authorization, and Accounting (AAA) infrastructure (e.g., Network Access Server and AAA server) also offers 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.

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

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 [6] scenarios, require the specification of a message exchange between the Home Agent (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 between the NAS and the AAA server needed in the split and integrated scenarios. Requirements are listed in case either IPsec or RFC 4285 [4] 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 the 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 [5], with the qualification that, unless otherwise stated, these words apply to the design of the AAA protocol extension, not its implementation or its usage.

The following terms are 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 set up 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 (e.g., Home Agent address as specified in [6]).

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 Mobility Service Authorizer (MSA) that stores user profiles and credentials.

4. Bootstrapping Scenarios

This section describes some bootstrapping scenarios in which communication between the AAA infrastructure of the Mobility Service Provider and the Home Agent is needed. The need of MIPv6-aware communication between the AAA server and the Network Access Server (NAS) is also described. The purpose of this section is only to explain the situation where bootstrapping is required. The actual mechanisms and additional details are specified elsewhere or are left for future work (see, e.g., [2], [3], and [6]).

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 [7] exchange with the HA to set up IPsec Security Associations (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 the 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 to check the validity of each MN's credentials with the AAA infrastructure, rather than having to maintain credentials for each MN itself. It also allows roaming in terms of Mobile IPv6 service where the MSP and MSA belong to different administrative domains. In this case, the HA in the MSP can check the validity of the credentials provided by the MN with the AAA infrastructure of MSA, receiving the relevant authorization information.

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 (in the 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, the assumption is that the Access Service Authorizer (ASA) is the same as the Mobility Service Authorizer (MSA). Further details of this type of a scenario are being worked on separately [6].

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

In this scenario, the 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 (the AAA server in the home network) sends the information about the assigned Home Agent to the 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, it passes Home Agent information received from the AAAH server to the DHCP server, for instance using mechanisms defined in [6].

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 mechanisms used to bootstrap the HoA, the IPsec Security Association, and the authentication and authorization with the MSA are the same as described in the bootstrapping solution for the 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 the split and integrated scenarios.

5.1. General Goals

G1.1 The communication between the AAAH server and the HA MUST reuse existing AAA security mechanisms with regard to authentication, replay, integrity, and confidentiality protection. These communication security mechanisms prevent a number of classical

threats, including the alteration of exchanged data (e.g., Mobile IPv6 configuration parameters) and the installation of unauthorized state.

5.2. Service Authorization

G2.1 The AAA-HA interface MUST allow the use of a 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 that the AAAH server grant an extension of the authorization lifetime 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 to the AAAH server 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 and MUST indicate that to the HA.

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

G2.10 The AAAH server MUST be able to support different levels of Mobile IPv6 authorization. For example, the AAAH server may authorize the MN to use MIPv6 (as defined in [1]) or may authorize the MN to utilize an IPv4 HoA assigned for Dual Stack MIPv6 [8].

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

G2.12 The HA MUST be able to authenticate the MN through the AAAH server in case a pre-shared 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 MUST support authentication based on the Mobility Message Authentication Options defined in [4].

G4.3 The AAAH server MUST be able to provide a MN-HA key (or data used for subsequent key derivation of the MN-HA key by the HA) to the HA if requested. Additional data, such as the Security Parameter Index (SPI) or lifetime parameters, are sent along with the keying material.

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

G4.5 The HA MUST include an identifier of the Mobile Node in the AAA transactions with the AAAH server.

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 server SHOULD be able to indicate to the HA if the MN is authorized to autoconfigure its Home Address. If the AAAH does not indicate to the HA if a MN is authorized to autoconfigure its address, the MN is not authorized.

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 operation 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 MUST be able to notify the AAAH server if it supports the AAA extensions designed to receive the HA assignment information.

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

8. Acknowledgements

The authors would like to thank James Kempf, Alper Yegin, Vijay Devarapalli, Basavaraj Patil, Gopal Dommety, Marcelo Bagnulo, 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 document. Finally the authors would like to thank Kuntal Chowdhury who contributed by identifying the goals related to RFC 4285 authentication.

9. References

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

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

9.2. Informative References

[6] Chowdhury, K., Ed., and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario", Work in Progress, April 2008.

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

[8] Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

Authors' Addresses

Gerardo Giaretta
Qualcomm
5775 Morehouse Drive
San Diego, CA 92109
USA

EMail: gerardo@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