Network Working Group
Request for Comments: 5030
Category: Informational

M. Nakhjiri, Ed.
Motorola
K. Chowdhury
Starent Networks
A. Lior
Bridgewater Systems
K. Leung
Cisco Systems

October 2007

Mobile IPv4 RADIUS Requirements

Status of This Memo

Abstract

This document provides an applicability statement as well as a scope definition for specifying Remote Authentication Dial-In User Service (RADIUS) extensions to support Mobile IPv4. The goal is to allow specification of RADIUS attributes to assist the Mobile IPv4 signaling procedures.

Table of Contents

1. Introduction

To kick start the Mobile IPv4 [RFC3344] processing of its packets by Mobile IP agents, a mobile node (MN) needs to be able to acquire a pair of home and care of addresses (HoA and CoA, respectively), find a willing agent to act as a Home Agent (HA) for the MN and perform a registration process with the HA. The registration process consists of an exchange of a registration request and a registration reply message between the MN and the HA. The specification in [RFC3344] allows an MN to start the registration process prior to having acquired its home address or the address of its HA. Acquiring those parameters by the MN is typically part of a process referred to as bootstrapping.

Successful processing of registration request and reply messages, among other things, depends on successful creation and verification of a number of authentication extensions developed specifically to protect the integrity and security of these messages and the entities processing them, i.e., MN, HA and some times, Foreign Agents (FAs) [RFC3344]. Creation as well as verification of these extensions requires existence of trust relationships and shared keys between MN and each of the mobility agents. However, creation of these trust relationships, typically referred to as mobility security associations (MSAs), is considered outside the scope of the base Mobile IPv4 specification defined in [RFC3344]. Avoiding the scalability issues arising from creating static security associations between an MN and all possible mobility agents is desired. Thus, establishing the associations dynamically, using the pre-existing relationship between the MN and the AAA server, is preferred.

To allow for utilization of an existing AAA infrastructure in the bootstrapping of the Mobile IPv4 parameters and security relationships, the Mobile IPv4 working group has developed Mobile IPv4 extensions to allow the MN to authenticate to the home AAA server [RFC4721]. The extensions also allow the MN to request assistance from the AAA server in creation of mobility security associations [RFC3957] with the mobility agents, using the pre-established trust relationship between the MN and its home AAA server.

While Mobile IPv4 extensions are necessary for implementing a utilization of the AAA infrastructure for Mobile IPv4 purposes, they are not sufficient. The interaction between the MN and the mobility agents (HA and FA) is based on Mobile IP signaling. However, the signaling beyond the mobility agents to the AAA server is typically based on AAA protocols. Around the time, when the specification of the aforementioned Mobile IP extensions was being developed, the AAA community was in the process of designing a successor to RADIUS.

Thus, the Mobile IP group developed a set of guidelines and requirements from the Mobile IP standpoint [RFC2977] specifically for such a successor (which turned out to be Diameter). These requirements led to the development of a specification for using Diameter in Mobile IPv4 bootstrapping [RFC4004]. The requirements for Mobile IP Authentication, Authorization, and Accounting [RFC2977] were standardized after the standardization of RADIUS [RFC2865].

Thus, it is obvious that RADIUS does not and cannot meet all the requirements listed in [RFC2977] without undergoing an extensive design change. Consequently, within IETF no RADIUS attributes have been standardized for Mobile IP support thus far. However, in the absence of IETF standardized RADIUS attributes, different wireless SDOs have taken the path of developing Vendor Specific Attributes (VSAs) for providing Mobile IPv4 support. The use of different vendor specific RADIUS attributes and procedures for the same purpose of Mobile IPv4 bootstrapping at different SDOs is deemed to cause a lack interoperability between these wireless standards, potentially hindering mobility across these wireless networks.

To respond to the described issue, it is desired to standardize a set of RADIUS attributes within IETF to allow a consistent and interoperable interaction with RADIUS based AAA infrastructure during the Mobile IPv4 Registration procedure. The bootstrapping attributes can include configuration parameters as well as material used for provisioning security of Mobile IPv4 messaging (authentication) as defined by [RFC4721] and [RFC3957].

As it stands today, RADIUS cannot meet all the requirements in [RFC2977]. The purpose of these requirements is to define a set of goals and non-goals specifically for RADIUS when it comes to assisting mobile nodes and mobility agents in bootstrapping Mobile IPv4 operation.

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 [RFC2119].

3. Goals and Non-Goals

Since this document serves as a requirement specification for RADIUS extensions that support Mobile IPv4 interaction with RADIUS infrastructure, the goals and non-goals refer to only those RADIUS extensions that are required to support Mobile IPv4.

3.1. Goals

The scope of the work is to standardize RADIUS attributes and to define the procedure by which the Mobile IPv4 agents (e.g., Home agent (HA) and Foreign Agent (FA)) map the Mobile IP registration message fields into the proposed RADIUS attributes, and vice versa.

- RADIUS servers are REQUIRED to be able to understand and process the attributes to be defined for Mobile IPv4 support and to perform verification of authentication extensions specified in [RFC4721]. RADIUS proxies are expected to be able to forward messages including the Mobile IPv4 related attributes as they would with any other RADIUS messages and attributes.

- All RADIUS work MUST be backward compatible with existing RADIUS RFCs, including RFCs the following: [RFC2865], [RFC2866], [RFC2867], [RFC2868], [RFC2869], [RFC3576], [RFC3579], and [RFC3580].

- Mobile IP agents (FA and HA) are REQUIRED to operate as RADIUS clients (NASes in context of [RFC2865]) when translating RADIUS signaling into Mobile IP signaling, and vice versa. Details on the behavior of Mobile IP agents as RADIUS clients are to be provided by the solution document describing the RADIUS extensions for Mobile IP support.

3.2. Non-Goals

The scope of this work is to only standardize RADIUS attributes and to define the procedure by which the Mobile IPv4 agents (e.g., Home agent (HA) and Foreign Agent (FA)) map the Mobile IP registration message fields into the proposed RADIUS attributes, and vice versa. Extension of the functionality of the existing protocol or RADIUS servers is not intended. More specifically, the following are NON-GOALS:

- Enhancing RADIUS Security: Creating new security properties for RADIUS, such as creating key transport capabilities is not the goal. No new security mechanisms are to be defined for the transport of RADIUS Access Requests in relation to the support of Mobile IPv4 bootstrapping. Existing RADIUS authentication procedures, e.g., Message-Authenticator (80) described in [RFC2869], are used. The security considerations for using RADIUS in bootstrapping Mobile IPv4 are described in a later section of this document.

- Enhancing RADIUS transport reliability: The transport properties of RADIUS remain intact. No new reliability mechanisms are defined in the transport of such Access Requests.

- Extending RADIUS message set: RADIUS extensions for bootstrapping Mobile IPv4 are not to define new RADIUS messages. The Diameter Mobile IP application [RFC4004] has defined new command codes to support Mobile IP signaling, depending on whether Diameter server is dealing with a Mobile IP HA or an FA. RADIUS currently does not have any messages that correspond to these Diameter commands. Instead, RADIUS extensions for Mobile IPv4 bootstrapping need to provide proposals for new RADIUS attributes that facilitate Diameter-RADIUS messaging translation without defining any new RADIUS messaging. At the same time, the RADIUS extensions for Mobile IPv4 need to re-use Diameter AVPs to the fullest extent possible.

- RFC 2977 compatibility: Extending RADIUS in a way that fulfills the full list of requirements in [RFC2977] will not be attempted.

4. Attributes

A specification of the RADIUS extensions for Mobile IPv4 needs to describe the full set of attributes required for RADIUS-Mobile IP interaction. While some of the attributes may already be standardized, others will require standardization and IANA type assignments.

5. IANA Considerations

This requirement document does not allocate any numbers, so there are no IANA considerations. On the other hand, future solution documents for RADIUS support of Mobile IPv4 will likely introduce new RADIUS attributes. Thus, those documents will need new attribute type numbers assigned by IANA.

6. Security Considerations

Enhancing security properties of RADIUS are a specific non-goal for the RADIUS extensions providing support for Mobile IP. Also, as this is a requirements document and not a solution specification document, no new security considerations are noted, aside from those that already exist for RADIUS. As such, the existing RADIUS security considerations described previously apply, and no additional security considerations are added here. For instance, the assumption in RADIUS is that intermediary nodes are trusted, while at the same time there is a concern on using AAA protocols that use hop-by-hop security to distribute keys. Use of hop-by-hop security for key

distribution can be in conflict with some of the requirements stated in [RFC4962], such as the requirement on binding a key to its context and the requirement on limitation of the key scope. The former for instance states that a key MUST be bound to the parties that are expected to have access to the keying material, while the latter implies that parties that do not require access to a key to perform their role MUST not have access to the key. Both of these requirements rule against trusting intermediary nodes and proxies with distribution of keys. Due to lack of end-to-end security mechanisms for RADIUS, imposing a MUST requirement for not trusting proxies is not possible. The RADIUS Extension working group is in the process of specifying procedures for wrapping key materials within RADIUS attributes. For the time being, support of Mobile IP within RADIUS may need to be based on trust of intermediaries, despite the security considerations described.

When it comes to protecting attributes in the Access Request, [RFC2868], Section 3.5 provides a mechanism for encrypting RADIUS attributes, such as passwords. There is also work under progress for specifying wrapping of sensitive attributes, such as key material within RADIUS Access Accept messages. This work is currently considered part of RADIUS crypto-agility extensions and when completed can be used in the process of distributing sensitive attributes, such as keying material from RADIUS servers.

It is also possible to protect RADIUS transactions using IPsec (e.g., as in RFC3579).

7. Acknowledgements

The authors would like to thank Alan DeKok for review and feedback, and Pete McCann and Jari Arkko for diligent shepherding of this document.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC2866] Rigney, C., "RADIUS Accounting", RFC 2866, June 2000.

[RFC2867] Zorn, G., Aboba, B., and D. Mitton, "RADIUS Accounting Modifications for Tunnel Protocol Support", RFC 2867, June 2000.

[RFC2977] Glass, S., Hiller, T., Jacobs, S., and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements", RFC 2977, October 2000.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3957] Perkins, C. and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4", RFC 3957, March 2005.

[RFC4004] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., and P. McCann, "Diameter Mobile IPv4 Application", RFC 4004, August 2005.

[RFC4721] Perkins, C., Calhoun, P., and J. Bharatia, "Mobile IPv4 Challenge/Response Extensions (Revised)", RFC 4721, January 2007.

[RFC4962] Housley, R. and B. Aboba, "Guidance for Authentication, Authorization, and Accounting (AAA) Key Management", BCP 132, RFC 4962, July 2007.

8.2. Informative References

[RFC2868] Zorn, G., Leifer, D., Rubens, A., Shriver, J., Holdrege, M., and I. Goyret, "RADIUS Attributes for Tunnel Protocol Support", RFC 2868, June 2000.

[RFC2869] Rigney, C., Willats, W., and P. Calhoun, "RADIUS Extensions", RFC 2869, June 2000.

[RFC3576] Chiba, M., Dommety, G., Eklund, M., Mitton, D., and B. Aboba, "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)", RFC 3576, July 2003.

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3580] Congdon, P., Aboba, B., Smith, A., Zorn, G., and J. Roese, "IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines", RFC 3580, September 2003.

Authors' Addresses

Madjid Nakhjiri (editor)
Motorola

EMail: madjid.nakhjiri@motorola.com

Kuntal Chowdhury
Starent Networks

EMail: kchowdhury@starentnetworks.com

Avi Lior
Bridgewater Systems

EMail: avi@bridgewatersystems.com

Kent Leung
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
US

EMail: kleung@cisco.com

Full Copyright Statement

Intellectual Property