IETF Mobile IPv6 Working Group
Internet Draft
Expires: August 2004

H. Ohnishi
M.Yanagiya
NTT
Y.Ohba
Toshiba

February 2004

Mobile IPv6 AAA Problem Statement

<draft-ohnishi-mip6-aaa-problem-statement-00.txt>

Status of this Memo

Abstract

Mobile IP achieves that Mobile Node(MN) moves from one subnet to another. If MN moves across different administrative domains in a commercial network, Mobile IPv6 requires AAA's support. This document describes the problem statement to use AAA functions in Mobile IPv6.

Conventions used in this document

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 [i].

Table of Contents

1. Introduction

Mobile IP(v4/v6) [RFC3344][I-D.ietf-mobileip-ipv6] achieves that Mobile Node (MN) moves from one subnet to another. If MN moves across different administrative domains where authentication, authorization and accounting (AAA) is always an issue especially in commercial-based deployments. Mobile IPv4 already defines an interface to AAA functionality [I-D.ietf-mip4-rfc3012bis] [I-D.ietf-aaa-diameter-mobileip] [I-D.ietf-mip4-aaa-nai]. Mobile IPv6 requires an interface to AAA as well. However such an interface has been a missing piece that needs to be filled with an appropriate solution.

This document describes several usage cases that deemed necessary to support when Mobile IPv6 is used in an environment where the users subscribe to commercial Mobile IPv6 services with credentials (username, password, certificate, etc.) that are used by the operators as the basis to perform the task of AAA for the Mobile IPv6 services.
The usage cases are described in terms of service bootstrapping and security, both are important in large-scale deployments. This document then addresses the fundamental issue that needs to be taken into account when designing an interface between AAA and Mobile IPv6. This document also contains informative description on the approach which is taken by Mobile IPv4 to support AAA, however, it should be noted that the informative description is not advocating or recommending the same approach adopted to Mobile IPv4 to be used for Mobile IPv6.

For more information related to IPv6 address assignment in 3GPP, it is recommended to read [RFC3314].

2. AAA usage scenario for Mobile IPv6

In this section, we show some application that we are going to solve by using AAA function. 2.1 shows the application to authenticate an MN when the MN accesses to the visiting network. From 2.2 to 2.4 shows service bootstrapping scenarios. Operators may choose a combination of scenarios from these for their services.

2.1 Roaming to foreign domain

Mobile IPv6 supports MN's mobility. But if MN moves to a foreign domain, the foreign domain requires the way of Authentication, Authorization and Accounting. RFC2977 shows requirements for this scheme. RFC2977 shows the applications of AAA to the Mobile IP, e.g. the basic model, the local payment model, the local home agent model and so on.

2.2 Dynamic home address prefix assignment via AAA

In some cases, operators want to assign home address prefix to mobile node dynamically for the purpose of reducing management cost, etc. Mobile IPv6 prescribes Mobile Prefix Solicitation(MPS) and Mobile Prefix Advertisement(MPA). But in this method, MN needs to know HA address previously. A solution for dynamically and securely assigning home address prefix to mobile node with involving an appropriate authentication and authorization protocol is demanded.

2.3 Dynamic HA address assignment via AAA

In some cases, operators want to assign HA to the MN dynamically from the perspective of load balancing. Mobile IPv6 prescribes dynamic HA allocation mechanism in which it sends anycast address to find HA and the HA sends back HAs' list to the MN. HA sends this list without authenticating the MN. A solution for dynamically and securely assigning HA's address to mobile node with involving an appropriate authentication and authorization protocol is demanded.

2.4 Bootstrapping Mobile IPv6 SA from AAA

Mobile IPv6 [I-D.ietf-mobileip-ipv6] requires an IPsec SA (Security Association) established between mobile node and its home agent to protect Binding Updates to the home agent. This SA is referred to as Mobile IPv6 SA(MSA). When a home agent is dynamically allocated, it is difficult to assume pre-established security association (such as an IKE [RFC2409] pre-shared secret) between the mobile node and every potential home agent, unless a trusted third-party is involved in the

authentication procedure between a mobile node and its home agent. Among several alternative models (e.g., Kerberos) that rely on a trusted third-party, there is demand for AAA-based solutions possibly with leveraging the EAP keying framework [I-D.ietf-eap-keying] which allows the key material generated by an EAP authentication algorithm to turn into a credential needed for mutually authenticating mobile node and home agent in the IPsec key management protocol.

3. Problem Statement

In Mobile IPv4, AAA for network access service and AAA for Mobile IPv4 service are integrated for optimization purpose. These two types of AAA are different in functionality [I-D.ietf-pana-usage-scenarios], and such an integration is possible in the architecture where an agent that acts as an AAA attendant for both types of AAA is placed in the visiting network. In the case of Mobile IPv4, mobility agent itself (i.e., FA) is such an integrated agent.

In Mobile IPv6 architecture, there is no FA unlike Mobile IPv4. The fundamental problem that needs to be solved is to support the usage cases described in Section 2 without introducing FA in Mobile IPv6. This would lead to a need to define a MIPv6 Service Aware AAA Attendant (MSAAA), which is an AAA attendant to provide AAA for Mobile IPv6 service for MN. The MSAAA may be integrated with an AAA attendant of other protocol or service, or may be integrated with MIPv6 home agent, depending on Mobile IPv6 service models. The protocol to transfer information between HA and AAA server is needed in every above MSAAA deployment scenarios.

4. Mobile IPv4 AAA solution (informative)

Mobile IPv4 defines two different registration procedures, one via foreign agent that relays the registration to mobile node's home agent, and the other directly with the mobile node's home agent. Both registration procedures involve the exchange of Registration Request and Registration Reply messages. In order to prevent spoofing, Mobile IPv4 defines authentication extension in Registration Request and Reply message [RFC3344]. MN sends Registration Request with authentication extension which includes authenticator to FA or HA. FA or HA evaluates the authenticator by using shared key or public/private key pair. In a large scale roaming service network such as public wireless LAN access service network, it is difficult to distribute all key material to FA and/or HA. Thus, AAA architecture is used to manage key materials of MNs or/and verify credential. Fig 1 shows an example of sequence using RADIUS. It is assumed that MN does not have a security association with FA. MN

sends Registration Request which includes challenge value and Network

Access Identifier (NAI). According to NAI, FA makes a decision on AAA message routing, and passes the authenticator to AAA server. AAA server verifies the authenticator and sends authentication reply. If an authentication is success, FA sends Agent Reply to MN.

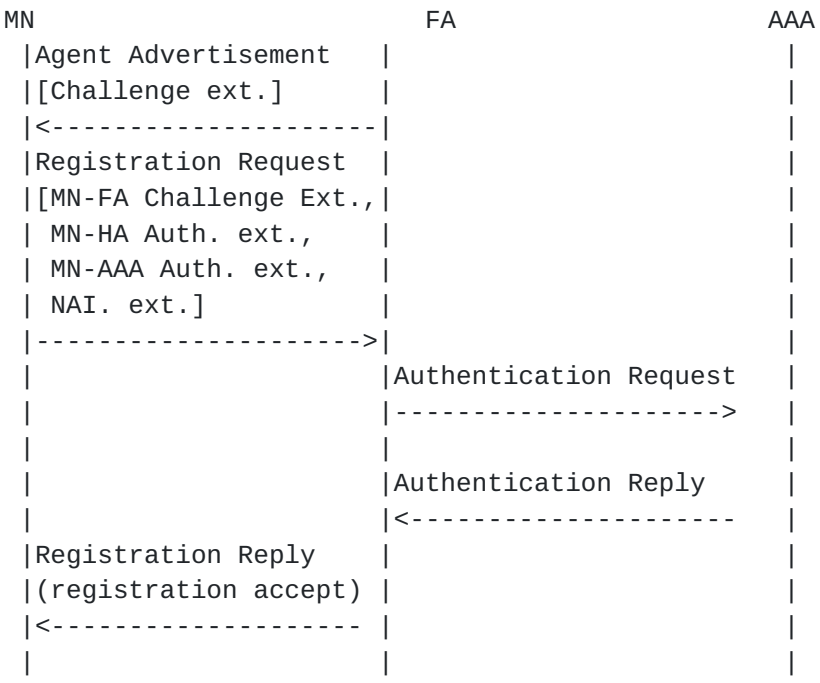

Figure 1: MN-FA authentication with AAA in Mobile IPv4

In [I-D.ietf-aaa-diameter-mobileip], a similar method is specified by using Diameter application. MN sends Registration Request to FA. FA invokes the local AAA infrastructure (AAAF) to request that a mobile node be authenticated. If AAAF is not aware of the identity of MN, AAAF will forward authentication data to home AAA server (AAAH).

5. Security Consideration

This draft identifies a need for bootstrapping Mobile IPv6 by leveraging the AAA infrastructure. Although any solution is not specified in this document, a AAA-based solution for dynamically assigning Mobile IPv6 home agent address is expected to improve Mobile IPv6 security by not relying on the anycast-based scheme built in Mobile IPv6 but relying on the AAA infrastructure instead. More security analysis on bootstrapping MSA should be made when designing a solution. Although security consideration section of [I-D.ietf-eap-keying] covers general security issues for EAP-based service bootstrapping, there may be Mobile IPv6 specific security issues in bootstrapping MSA.

Reference

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

[I-D.ietf-mobileip-ipv6] Johnson, D., "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24.txt, (work in progress), June 30 2003.

[I-D.ietf-mip4-rfc3012bis] C. Perkins, et al., "Mobile IPv4 Challenge/Response Extensions (revised)", draft-ietf-mip4-rfc3012bis-00.txt (work in progress), 7 October 2003.

[I-D.ietf-aaa-diameter-mobileip] P. Calhoun, et al., "Diameter Mobile IP Application", draft-ietf-aaa-diameter-mobileip-15.txt (work in progress), November 2003.

[I-D.ietf-mip4-aaa-nai] F. Johansson and T. Johansson, "Mobile IPv4 Extension for carrying Network Access Identifiers", draft-ietf-mip4-aaa-nai-02.txt (work in progress), December 12, 2003

[RFC3314] M. Wasserman, "Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards", RFC 3314, September 2002.

[I-D.ietf-pana-usage-scenarios] Y. Ohba, et al., "Problem Statement and Usage Scenarios for PANA", draft-ietf-pana-usage-scenarios-06.txt (work in progress), April 28, 2003.

[RFC2977] S. Glass, et al.,"Mobile IP Authentication, Authorization, and Accounting Requirements", RFC 2977, October 2000

[RFC2409] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[I-D.ietf-eap-keying] Aboba, B., "EAP Key Management Framework", draft-ietf-eap-keying-01 (work in progress), October 2003.

[I-D.ietf-ipsec-ikev2] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", draft-ietf-ipsec-ikev2-12 (work in progress), January 2004.

Acknowledgments

We would like to thank Alper Yegin and Rafa Marin Lopez for their valuable contributions to the discussions and preparation of this document.

We also would like to thank Basavaraj Patil and Gopal Dommety for their encouraging us to submit this document.

Author's Addresses

Hiroyuki Ohnishi
NTT Network service systems laboratories, NTT Corporation
9-11, Midori-Cho, 3-Chome
Musashino-Shi, Tokyo 180-8585
Japan
Phone: +81 422 59 4132
Email: ohnishi.hiroyuki@lab.ntt.co.jp

Mayumi Yanagiya
NTT Network service systems laboratories, NTT Corporation
9-11, Midori-Cho, 3-Chome
Musashino-Shi, Tokyo 180-8585
Japan
Phone: +81 422 59 6783
Email: yanagiya.mayumi @lab.ntt.co.jp

Yoshihiro Ohba
Toshiba America Information Systems, Inc.
9740 Irvine Blvd.
Irvine, CA 92619-1697
USA
Phone: +1 973 829 5174
EMail: yohba@tari.toshiba.com