Network Working Group
Request for Comments: 4283
Category: Standards Track

A. Patel
K. Leung
Cisco Systems
M. Khalil
H. Akhtar
Nortel Networks
K. Chowdhury
Starent Networks

November 2005

Mobile Node Identifier Option for Mobile IPv6 (MIPv6)

Status of This Memo

Copyright Notice

Abstract

Mobile IPv6 (MIPv6) defines a new Mobility header that is used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings. Mobile IPv6 nodes need the capability to identify themselves using an identity other than the default home IP address. Some examples of identifiers include Network Access Identifier (NAI), Fully Qualified Domain Name (FQDN), International Mobile Station Identifier (IMSI), and Mobile Subscriber Number (MSISDN). This document defines a new mobility option that can be used by Mobile IPv6 entities to identify themselves in messages containing a mobility header.

Table of Contents

1. Introduction

The base specification of Mobile IPv6 [RFC3775] identifies mobility entities using an IPv6 address. It is essential to have a mechanism wherein mobility entities can be identified using other identifiers (for example, a Network Access Identifier (NAI) [RFC4282], International Mobile Station Identifier (IMSI), or an application/ deployment specific opaque identifier).

The capability to identify a mobility entity via identifiers other than the IPv6 address can be leveraged for performing various functions, for example,

- authentication and authorization using an existing AAA (Authentication, Authorization, and Accounting) infrastructure or via an HLR/AuC (Home Location Register/Authentication Center)

- dynamic allocation of a mobility anchor point

- dynamic allocation of a home address

This document defines an option with a subtype number that denotes a specific type of identifier. One instance of subtype, the NAI, is defined in Section 3.1. It is anticipated that other identifiers will be defined for use in the mobility header in the future.

This option SHOULD be used when Internet Key Exchange (IKE)/IPsec is not used for protecting binding updates or binding acknowledgements as specified in [RFC3775]. It is typically used with the authentication option [RFC4285]. But this option may be used independently. For example, the identifier can provide accounting and billing services.

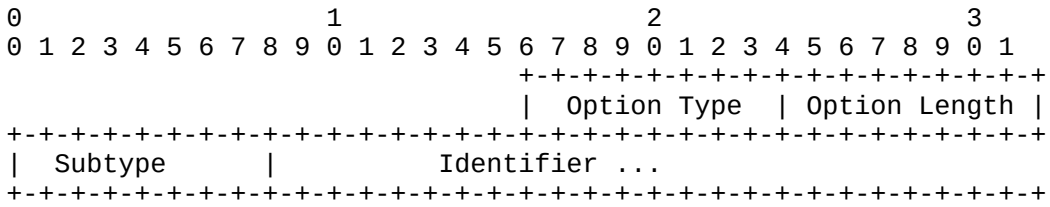
2. Terminology

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Mobile Node Identifier Option

The Mobile Node Identifier option is a new optional data field that is carried in the Mobile IPv6-defined messages that includes the Mobility header. Various forms of identifiers can be used to identify a Mobile Node (MN). Two examples are a Network Access Identifier (NAI) [RFC4282] and an opaque identifier applicable to a particular application. The Subtype field in the option defines the specific type of identifier.

This option can be used in mobility messages containing a mobility header. The subtype field in the option is used to interpret the specific type of identifier.



Option Type:

MN-ID-OPTION-TYPE has been assigned value 8 by the IANA. It is an 8-bit identifier of the type mobility option.

Option Length:

8-bit unsigned integer, representing the length in octets of the Subtype and Identifier fields.

Subtype:

Subtype field defines the specific type of identifier included in the Identifier field.

Identifier:

A variable length identifier of type, as specified by the Subtype field of this option.

This option does not have any alignment requirements.

3.1. MN-NAI Mobility Option

The MN-NAI mobility option uses the general format of the Mobile Node Identifier option as defined in Section 3. This option uses the subtype value of 1. The MN-NAI mobility option is used to identify the mobile node.

The MN-NAI mobility option uses an identifier of the form user@realm [RFC4282]. This option MUST be implemented by the entities implementing this specification.

3.2. Processing Considerations

The location of the MN Identifier option is as follows: When present, this option MUST appear before any authentication-related option in a message containing a Mobility header.

4. Security Considerations

4.1. General Considerations

Mobile IPv6 already contains one mechanism for identifying mobile nodes, the Home Address option [RFC3775]. As a result, the vulnerabilities of the new option defined in this document are similar to those that already exist for Mobile IPv6. In particular, the use of a permanent, stable identifier may compromise the privacy of the user, making it possible to track a particular device or user as it moves through different locations.

4.2. MN-NAI Considerations

Since the Mobile Node Identifier option described in Section 3 reveals the home affiliation of a user, it may assist an attacker in determining the identity of the user, help the attacker in targeting specific victims, or assist in further probing of the username space.

These vulnerabilities can be addressed through various mechanisms, such as those discussed below:

- Encrypting traffic at the link layer, such that other users on the same link do not see the identifiers. This mechanism does not help against attackers on the rest of the path between the mobile node and its home agent.

- Encrypting the whole packet, such as when using IPsec to protect the communications with the home agent [RFC3776].

- Using an authentication mechanism that enables the use of privacy NAIs [RFC4282] or temporary, changing "pseudonyms" as identifiers.

In any case, it should be noted that as the identifier option is only needed on the first registration at the home agent and subsequent registrations can use the home address, the window of privacy vulnerability in this document is reduced as compared to [RFC3775]. In addition, this document is a part of a solution to allow dynamic home addresses to be used. This is an improvement to privacy as well, and it affects both communications with the home agent and the correspondent nodes, both of which have to be told the home address.

5. IANA Considerations

The values for new mobility options must be assigned from the Mobile IPv6 [RFC3775] numbering space.

The IANA has assigned the value 8 for the MN-ID-OPTION-TYPE.

In addition, IANA has created a new namespace for the subtype field of the Mobile Node Identifier option. The currently allocated values are as follows:

NAI (defined in [RFC4282]).

New values for this namespace can be allocated using Standards Action [RFC2434].

6. Acknowledgements

The authors would like to thank Basavaraj Patil for his review and suggestions on this document. Thanks to Jari Arkko for review and suggestions regarding security considerations and various other aspects of the document.

7. Normative References

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

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3776] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.

[RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, November 2005.

8. Informative Reference

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, November 2005.

Authors' Addresses

Alpesh Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US

Phone: +1 408-853-9580
EMail: alpesh@cisco.com

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

Phone: +1 408-526-5030
EMail: kleung@cisco.com

Mohamed Khalil
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US

Phone: +1 972-685-0574
EMail: mkhalil@nortel.com

Haseeb Akhtar
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US

Phone: +1 972-684-4732
EMail: haseebak@nortel.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
US

Phone: +1 214 550 1416
EMail: kchowdhury@starentnetworks.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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