Network Working Group
Request for Comments: 4285
Category: Informational

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

January 2006

Authentication Protocol for Mobile IPv6

Status of this Memo

Copyright Notice

IESG Note

This RFC is not a candidate for any level of Internet Standard. RFC 3775 and 3776 define Mobile IPv6 and its security mechanism. This document presents an alternate security mechanism for Mobile IPv6 used in 3GPP2 networks.

The security properties of this mechanism have not been reviewed in the IETF. Conducting this review proved difficult because the standards-track security mechanism for Mobile IPv6 is tightly integrated into the protocol; extensions to Mobile IPv6 and the core documents make assumptions about the properties of the security model without explicitly stating what assumptions are being made. There is no documented service model. Thus it is difficult to replace the security mechanism and see if the current protocol and future extensions meet appropriate security requirements both under the original and new security mechanisms. If a service model for Mobile IPv6 security is ever formally defined and reviewed, a mechanism similar to this one could be produced and fully reviewed.

Section 1.1 of this document provides an applicability statement for this RFC. The IESG recommends against the usage of this specification outside of environments that meet the conditions of that applicability statement. In addition the IESG recommends those

considering deploying or implementing this specification conduct a sufficient security review to meet the conditions of the environments in which this RFC will be used.

Abstract

IPsec is specified as the means of securing signaling messages between the Mobile Node and Home Agent for Mobile IPv6 (MIPv6). MIPv6 signaling messages that are secured include the Binding Updates and Acknowledgement messages used for managing the bindings between a Mobile Node and its Home Agent. This document proposes an alternate method for securing MIPv6 signaling messages between Mobile Nodes and Home Agents. The alternate method defined here consists of a MIPv6-specific mobility message authentication option that can be added to MIPv6 signaling messages.

Table of Contents

1. Introduction

The base Mobile IPv6 specification [RFC3775] specifies the signaling messages, Binding Update (BU) and Binding Acknowledgement (BA), between the Mobile Node (MN) and Home Agent (HA) to be secured by the IPsec Security Associations (IPsec SAs) that are established between these two entities.

This document proposes a solution for securing the Binding Update and Binding Acknowledgment messages between the Mobile Node and Home Agent using a mobility message authentication option that is included in these messages. Such a mechanism enables IPv6 mobility in a host without having to establish an IPsec SA with its Home Agent. A Mobile Node can implement Mobile IPv6 without having to integrate it with the IPsec module, in which case the Binding Update and Binding Acknowledgement messages (between MN-HA) are secured with the mobility message authentication option.

The authentication mechanism proposed here is similar to the authentication mechanism used in Mobile IPv4 [RFC3344].

1.1. Applicability Statement

The mobility message authentication option specified in Section 5 is applicable in certain types of networks that have the following characteristics:

- Networks in which the authentication of the MN for network access is done by an authentication server in the home network via the home agent. The security association is established by the network operator (provisioning methods) between the MN and a backend authentication server (e.g., Authentication, Authorization, and Accounting (AAA) home server). MIPv6 as per RFCs 3775 and 3776 relies on the IPsec SA between the MN and an HA. In cases where the assignment of the HA is dynamic and the only static or long-term SA is between the MN and a backend authentication server, the mobility message authentication option is desirable.

- In certain deployment environments, the mobile node needs dynamic assignment of a home agent and home address. The assignment of such can be on a per-session basis or on a per-MN power-up basis. In such scenarios, the MN relies on an identity such as a Network Access Identifier (NAI) [RFC4283], and a security association with a AAA server to obtain such bootstrapping information. The security association is created via an out-of-band mechanism or by non Mobile IPv6 signaling. The out-of-band mechanism can be specific to the deployment environment of a network operator. In Code Division Multiple Access (CDMA) network deployments, this information can be

obtained at the time of network access authentication via [3GPP2] specific extensions to PPP or DHCPv6 on the access link and by AAA extensions in the core. It should be noted that the out-of-band mechanism is not within the scope of the mobility message authentication option (Section 5) and hence is not described therein.

- Network deployments in which not all Mobile Nodes and Home Agents have IKEv2 implementations and support for the integration of IKEv2 with backend AAA infrastructures. IKEv2 as a technology has yet to reach maturity status and widespread implementations needed for commercial deployments on a large scale. At the time of this writing, [RFC4306] is yet to be published as an RFC. Hence from a practical perspective that operators face, IKEv2 is not yet capable of addressing the immediate need for MIPv6 deployment.

- Networks that expressly rely on the backend AAA infrastructure as the primary means for identifying and authentication/authorizing a mobile user for MIPv6 service.

- Networks in which the establishment of the security association between the Mobile Node and the authentication server (AAA Home) is established using an out-of-band mechanism and not by any key exchange protocol. Such networks will also rely on out-of-band mechanisms to renew the security association (between MN and AAA Home) when needed.

- Networks that are bandwidth constrained (such as cellular wireless networks) and for which there exists a strong desire to minimize the number of signaling messages sent over such interfaces. MIPv6 signaling that relies on Internet Key Exchange (IKE) as the primary means for setting up an SA between the MN and HA requires more signaling messages compared with the use of an mobility message authentication option carried in the BU/BA messages.

One such example of networks that have such characteristics are CDMA networks as defined in [3GPP2].

2. Overview

This document presents a lightweight mechanism to authenticate the Mobile Node at the Home Agent or at the Authentication, Authorization, and Accounting (AAA) server in Home network (AAAH) based on a shared-key-based mobility security association between the Mobile Node and the respective authenticating entity. This shared-key-based mobility security association (shared-key-based mobility SA) may be statically provisioned or dynamically created. The term

"mobility security association" referred to in this document is understood to be a "shared-key-based Mobile IPv6 authentication" security association.

This document introduces new mobility options to aid in authentication of the Mobile Node to the Home Agent or AAAH server. The confidentiality protection of Return Routability messages and authentication/integrity protection of Mobile Prefix Discovery (MPD) is not provided when these options are used for authentication of the Mobile Node to the Home Agent. Thus, unless the network can guarantee such protection (for instance, like in 3GPP2 networks), Route Optimization and Mobile Prefix Discovery should not be used when using the mobility message authentication option.

3. 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 RFC 2119.

3.1. General Terms

First (size, input)

Some formulas in this specification use a functional form "First (size, input)" to indicate truncation of the "input" data so that only the first "size" bits remain to be used.

Shared-key-based Mobility Security Association

Security relation between the Mobile Node and its Home Agent, used to authenticate the Mobile Node for mobility service. The shared-key-based mobility security association between Mobile Node and Home Agent consists of a mobility Security Parameter Index (SPI), a shared key, an authentication algorithm, and the replay protection mechanism in use.

Mobility SPI

A number in the range [0-4294967296] used to index into the shared-key-based mobility security associations.

4. Operational Flow

The figure below describes the sequence of messages sent and received between the MN and HA in the registration process. Binding Update (BU) and Binding Acknowledgement (BA) messages are used in the registration process.

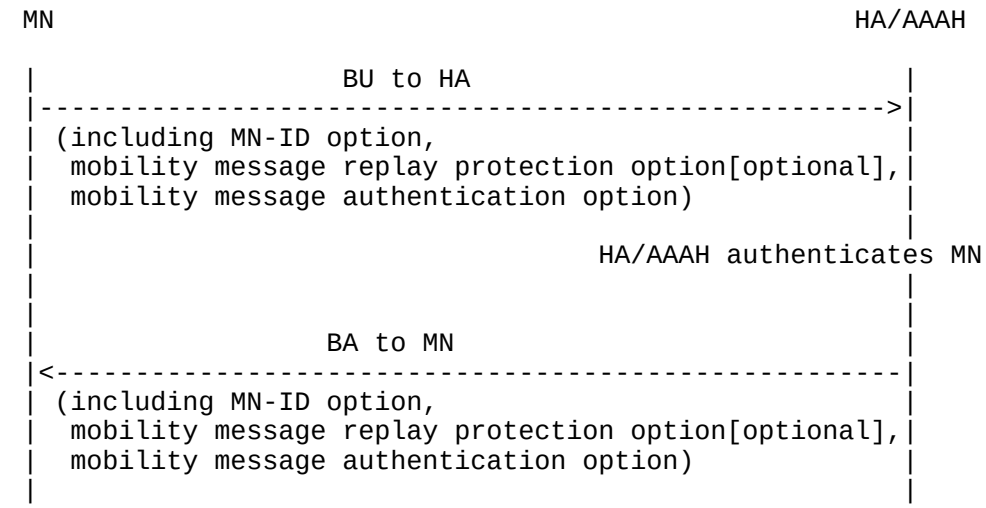

Figure 1: Home Registration with Authentication Protocol

The Mobile Node MUST use the Mobile Node Identifier option, specifically the MN-NAI mobility option as defined in [RFC4283] to identify itself while authenticating with the Home Agent. The Mobile Node uses the Mobile Node Identifier option as defined in [RFC4283] to identify itself as may be required for use with some existing AAA infrastructure designs.

The Mobile Node MAY use the Message Identifier option as defined in Section 6 for additional replay protection.

The mobility message authentication option described in Section 5 may be used by the Mobile Node to transfer authentication data when the Mobile Node and the Home Agent are utilizing a mobility SPI (a number in the range [0-4294967296] used to index into the shared-key-based mobility security associations) to index between multiple mobility security associations.

5. Mobility Message Authentication Option

This section defines a mobility message authentication option that may be used to secure Binding Update and Binding Acknowledgement messages. This option can be used along with IPsec or preferably as an alternate mechanism to authenticate Binding Update and Binding Acknowledgement messages in the absence of IPsec.

This document also defines subtype numbers, which identify the mode of authentication and the peer entity to authenticate the message. Two subtype numbers are specified in this document. Other subtypes may be defined for use in the future.

Only one instance of a mobility message authentication option of a particular subtype can be present in the message. One message may contain multiple instances of the mobility message authentication option with different subtype values. If both MN-HA and MN-AAA authentication options are present, the MN-HA authentication option must be present before the MN-AAA authentication option (else, the HA MUST discard the message).

When a Binding Update or Binding Acknowledgement is received without a mobility message authentication option and the entity receiving it is configured to use the mobility message authentication option or has the shared-key-based mobility security association for the mobility message authentication option, the entity should silently discard the received message.

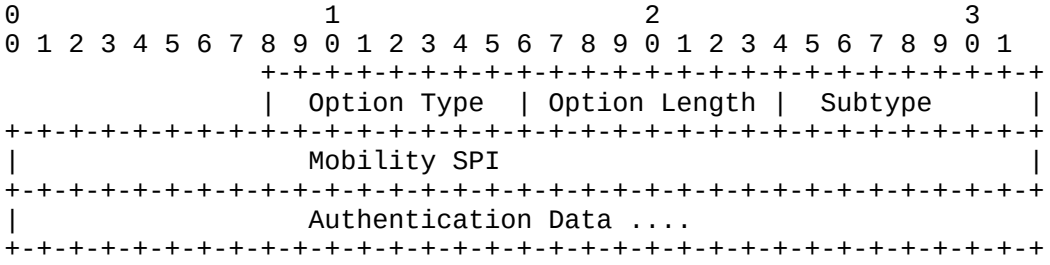

Figure 2: Mobility Message Authentication Option

Option Type:

AUTH-OPTION-TYPE value 9 has been defined by IANA. An 8-bit identifier of the type mobility option.

Option Length:

8-bit unsigned integer, representing the length in octets of the Subtype, mobility Security Parameter Index (SPI) and Authentication Data fields.

Subtype:

A number assigned to identify the entity and/or mechanism to be used to authenticate the message.

Mobility SPI:

Mobility Security Parameter Index

Authentication Data:

This field has the information to authenticate the relevant mobility entity. This protects the message beginning at the Mobility Header up to and including the mobility SPI field.

Alignment requirements :

The alignment requirement for this option is 4n + 1.

5.1. MN-HA Mobility Message Authentication Option

The format of the MN-HA mobility message authentication option is as defined in Figure 2. This option uses the subtype value of 1. The MN-HA mobility message authentication option is used to authenticate the Binding Update and Binding Acknowledgement messages based on the shared-key-based security association between the Mobile Node and the Home Agent.

The shared-key-based mobility security association between Mobile Node and Home Agent used within this specification consists of a mobility SPI, a key, an authentication algorithm, and the replay protection mechanism in use. The mobility SPI is a number in the range [0-4294967296], where the range [0-255] is reserved. The key consists of an arbitrary value and is 16 octets in length. The authentication algorithm is HMAC_SHA1. The replay protection mechanism may use the Sequence number as specified in [RFC3775] or the Timestamp option as defined in Section 6. If the Timestamp option is used for replay protection, the mobility security association includes a "close enough" field to account for clock drift. A default value of 7 seconds SHOULD be used. This value SHOULD be greater than 3 seconds.

The MN-HA mobility message authentication option MUST be the last option in a message with a mobility header if it is the only mobility message authentication option in the message.

The authentication data is calculated on the message starting from the mobility header up to and including the mobility SPI value of this option.

Authentication Data = First (96, HMAC_SHA1(MN-HA Shared key, Mobility Data))

Mobility Data = care-of address | home address | Mobility Header (MH) Data

MH Data is the content of the Mobility Header up to and including the mobility SPI field of this option. The Checksum field in the Mobility Header MUST be set to 0 to calculate the Mobility Data.

The first 96 bits from the Message Authentication Code (MAC) result are used as the Authentication Data field.

5.1.1. Processing Considerations

The assumption is that the Mobile Node has a shared-key-based security association with the Home Agent. The Mobile Node MUST include this option in a BU if it has a shared-key-based mobility security association with the Home Agent. The Home Agent MUST include this option in the BA if it received this option in the corresponding BU and Home Agent has a shared-key-based mobility security association with the Mobile Node.

The Mobile Node or Home Agent receiving this option MUST verify the authentication data in the option. If authentication fails, the Home Agent MUST send BA with Status Code MIPV6-AUTH-FAIL. If the Home Agent does not have shared-key-based mobility SA, Home Agent MUST discard the BU. The Home Agent MAY log such events.

5.2. MN-AAA Mobility Message Authentication Option

The format of the MN-AAA mobility message authentication option is as defined in Figure 2. This option uses the subtype value of 2. The MN-AAA authentication mobility option is used to authenticate the Binding Update message based on the shared mobility security association between the Mobile Node and AAA server in Home network (AAAH). It is not used in Binding Acknowledgement messages. The corresponding Binding Acknowledgement messages must be authenticated using the MN-HA mobility message authentication option (Section 5.1).

The MN-AAA mobility message authentication option must be the last option in a message with a mobility header. The corresponding response MUST include the MN-HA mobility message authentication option, and MUST NOT include the MN-AAA mobility message authentication option.

The Mobile Node MAY use the Mobile Node Identifier option [RFC4283] to enable the Home Agent to make use of available AAA infrastructure.

The authentication data is calculated on the message starting from the mobility header up to and including the mobility SPI value of this option.

The authentication data shall be calculated as follows:

Authentication data = hash_fn(MN-AAA Shared key, MAC_Mobility Data)

hash_fn() is decided by the value of mobility SPI field in the MN-AAA mobility message authentication option.

SPI = HMAC_SHA1_SPI:

If mobility SPI has the well-known value HMAC_SHA1_SPI, then hash_fn() is HMAC_SHA1. When HMAC_SHA1_SPI is used, the BU is authenticated by AAA using HMAC_SHA1 authentication. In that case, MAC_Mobility Data is calculated as follows:

MAC_Mobility Data = SHA1(care-of address | home address | MH Data)

MH Data is the content of the Mobility Header up to and including the mobility SPI field of this option.

5.2.1. Processing Considerations

The use of the MN-AAA mobility message authentication option assumes that AAA entities at the home site communicate with the HA via an authenticated channel. Specifically, a BU with the MN-AAA mobility message authentication option is authenticated via a home AAA server. The specific details of the interaction between the HA and the AAA server is beyond the scope of this document.

When the Home Agent receives a Binding Update with the MN-AAA mobility message authentication option, the Binding Update is authenticated by an entity external to the Home Agent, typically a AAA server.

5.3. Authentication Failure Detection at the Mobile Node

In case of authentication failure, the Home Agent MUST send a Binding Acknowledgement with status code MIPV6-AUTH-FAIL to the Mobile Node, if a shared-key-based mobility security association to be used between Mobile Node and Home Agent for authentication exists. If there is no shared-key-based mobility security association, HA drops the Binding Update. HA may log the message for administrative action.

Upon receiving a Binding Acknowledgement with status code MIPV6-AUTH-FAIL, the Mobile Node SHOULD stop sending new Binding Updates to the Home Agent.

6. Mobility Message Replay Protection Option

The Mobility message replay protection option MAY be used in Binding Update/Binding Acknowledgement messages when authenticated using the mobility message authentication option as described in Section 5.

The mobility message replay protection option is used to let the Home Agent verify that a Binding Update has been freshly generated by the Mobile Node and not replayed by an attacker from some previous Binding Update. This is especially useful for cases where the Home Agent does not maintain stateful information about the Mobile Node after the binding entry has been removed. The Home Agent does the replay protection check after the Binding Update has been authenticated. The mobility message replay protection option when included is used by the Mobile Node for matching BA with BU.

If this mode of replay protection is used, it needs to be part of the shared-key-based mobility security association.

If the policy at Home Agent mandates replay protection using this option (as opposed to the sequence number in the Mobility Header in Binding Update) and the Binding Update from the Mobile Node does not include this option, the Home Agent discards the BU and sets the Status Code in BA to MIPV6-MESG-ID-REQD.

When the Home Agent receives the mobility message replay protection option in Binding Update, it MUST include the mobility message replay protection option in Binding Acknowledgement. Appendix A provides details regarding why the mobility message replay protection option MAY be used when using the authentication option.

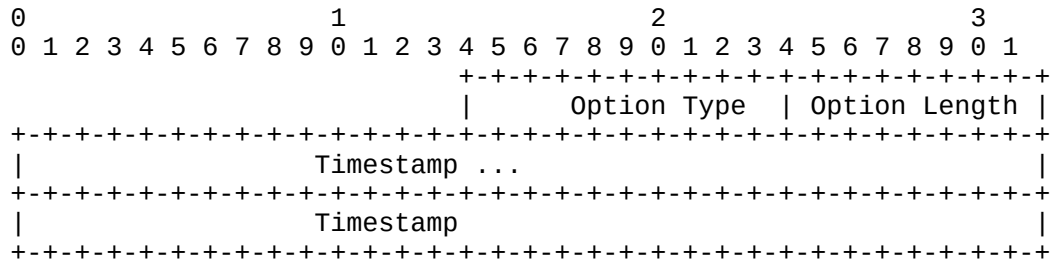

Figure 3: Mobility Message Replay Protection Option

Option Type:

MESG-ID-OPTION-TYPE value 10 has been defined by IANA. An 8-bit identifier of the type mobility option.

Option Length:

8-bit unsigned integer, representing the length in octets of the Timestamp field.

Timestamp:

This field carries the 64 bit timestamp.

Alignment requirements :

The alignment requirement for this option is 8n + 2.

The basic principle of timestamp replay protection is that the node generating a message inserts the current time of day, and the node receiving the message checks that this timestamp is sufficiently close to its own time of day. Unless specified differently in the shared-key-based mobility security association between the nodes, a default value of 7 seconds MAY be used to limit the time difference. This value SHOULD be greater than 3 seconds. The two nodes must have adequately synchronized time-of-day clocks.

The Mobile Node MUST set the Timestamp field to a 64-bit value formatted as specified by the Network Time Protocol (NTP) [RFC1305]. The low-order 32 bits of the NTP format represent fractional seconds, and those bits that are not available from a time source SHOULD be generated from a good source of randomness. Note, however, that when using timestamps, the 64-bit timestamp used in a Binding Update from the Mobile Node MUST be greater than that used in any previous successful Binding Update.

After successful authentication of Binding Update (either locally at the Home Agent or when a success indication is received from the AAA server), the Home Agent MUST check the Timestamp field for validity. In order to be valid, the timestamp contained in the Timestamp field MUST be close enough to the Home Agent's time-of-day clock and the timestamp MUST be greater than all previously accepted timestamps for the requesting Mobile Node.

If the timestamp is valid, the Home Agent copies the entire Timestamp field into the Timestamp field in the BA it returns to the Mobile Node. If the timestamp is not valid, the Home Agent copies only the low-order 32 bits into the BA, and supplies the high-order 32 bits from its own time of day.

If the Timestamp field is not valid but the authentication of the BU succeeds, the Home Agent MUST send a Binding Acknowledgement with status code MIPV6-ID-MISMATCH. The Home Agent does not create a binding cache entry if the timestamp check fails.

If the Mobile Node receives a Binding Acknowledgement with the code MIPV6-ID-MISMATCH, the Mobile Node MUST authenticate the BA by processing the MN-HA authentication mobility option.

If authentication succeeds, the Mobile Node MUST adjust its timestamp and send subsequent Binding Update using the updated value.

Upon receiving a BA that does not contain the MIPV6-ID-MISMATCH status code, the Mobile Node MUST compare the Timestamp value in the BA to the Timestamp value it sent in the corresponding BU. If the values match, the Mobile Node proceeds to process the MN-HA authentication data in the BA. If the values do not match, the Mobile Node silently discards the BA.

7. Security Considerations

This document proposes new mobility message authentication options to authenticate the control message between Mobile Node, Home Agent, and/or home AAA (as an alternative to IPsec). The new options provide for authentication of Binding Update and Binding Acknowledgement messages. The MN-AAA mobility message authentication option provide for authentication with AAA infrastructure.

This specification also introduces an optional replay protection mechanism in Section 6, to prevent replay attacks. The sequence number field in the Binding Update is not used if this mechanism is used. This memo defines the timestamp option to be used for mobility message replay protection.

8. IANA Considerations

IANA services are required for this specification. The values for new mobility options and status codes must be assigned from the Mobile IPv6 [RFC3775] numbering space.

The values for Mobility Option types AUTH-OPTION-TYPE and MESG-ID-OPTION-TYPE, as defined in Section 5 and Section 6, have been assigned. The values are 9 for the AUTH-OPTION-TYPE and 10 for the MESG-ID-OPTION-TYPE Mobility Option.

The values for status codes MIPV6-ID-MISMATCH, MIPv6-AUTH-FAIL, and MIPV6-MESG-ID-REQD, as defined in Section 6 and Section 5.3, have been assigned. The values are 144 for MIPV6-ID-MISMATCH 145 for MIPV6-MESG-ID-REQD and 146 for MIPV6-AUTH-FAIL.

A new section for enumerating algorithms identified by specific mobility SPIs within the range 0-255 has to be added to

http://www.iana.org/assignments/mobility-parameters

The currently defined values are as follows:

The value 0 should not be assigned.

The value 3 is reserved for HMAC_SHA1_SPI as defined in Section 5.2.

The value 5 is reserved for use by 3GPP2.

New values for this namespace can be allocated using IETF Consensus. [RFC2434].

In addition, IANA has created a new namespace for the Subtype field of the MN-HA and MN-AAA mobility message authentication options under

http://www.iana.org/assignments/mobility-parameters

The currently allocated values are as follows:

1 MN-HA mobility message authentication option Section 5.1

2 MN-AAA mobility message authentication option Section 5.2

New values for this namespace can be allocated using IETF Consensus. [RFC2434].

9. Acknowledgements

The authors would like to thank Basavaraj Patil, Charlie Perkins, Vijay Devarapalli, Jari Arkko, and Gopal Dommety, and Avi Lior for their thorough review and suggestions on the document. The authors would like to acknowledge the fact that a similar authentication method was considered in base protocol [RFC3775] at one time.

10. References

10.1. Normative References

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6", RFC 4283, November 2005.

[RFC1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

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

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

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

10.2. Informative References

[3GPP2] "cdma2000 Wireless IP Network Standard", 3GPP2 X.S0011-D, September 2005.

[RFC4306] Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

Appendix A. Rationale for Mobility Message Replay Protection Option

Mobile IPv6 [RFC3775] defines a Sequence Number in the mobility header to prevent replay attacks. There are two aspects that stand out in regards to using the Sequence Number to prevent replay attacks.

First, the specification states that the Home Agent should accept a BU with a Sequence Number greater than the Sequence Number from the previous Binding Update. This implicitly assumes that the Home Agent has some information regarding the Sequence Number from the previous BU (even when the binding cache entry is not present). Second, the specification states that if the Home Agent has no binding cache entry for the indicated home address, it MUST accept any Sequence Number value in a received Binding Update from this Mobile Node.

With the mechanism defined in this document, it is possible for the Mobile Node to register with a different Home Agent during each mobility session. Thus, it is unreasonable to expect each Home Agent in the network to maintain state about the Mobile Node. Also, if the Home Agent does not cache information regarding sequence number, as per the second point above, a replayed BU can cause a Home Agent to create a binding cache entry for the Mobile Node. Thus, when authentication option is used, Sequence Number does not provide protection against replay attack.

One solution to this problem (when the Home Agent does not save state information for every Mobile Node) would be for the Home Agent to reject the first BU and assign a (randomly generated) starting sequence number for the session and force the Mobile Node to send a fresh BU with the suggested sequence number. While this would work in most cases, it would require an additional round trip, and this extra signaling and latency is not acceptable in certain deployments [3GPP2]. Also, this rejection and using sequence number as a nonce in rejection is a new behavior that is not specified in [RFC3775].

Thus, this specification uses the mobility message replay protection option to prevent replay attacks. Specifically, timestamps are used to prevent replay attacks as described in Section 6.

It is important to note that as per Mobile IPv6 [RFC3775] this problem with sequence number exists. Since the base specification mandates the use of IPsec (and naturally that goes with IKE in most cases), the real replay protection is provided by IPsec/IKE. In case of BU/BA between Mobile Node and Client Node (CN), the liveness proof is provided by the use of nonces that the CN generates.

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 provided by the IETF Administrative Support Activity (IASA).