Network Working Group
Internet-Draft
Expires: December 31, 2004

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

July 2, 2004

Authentication Protocol for Mobile IPv6
draft-ietf-mip6-auth-protocol-00.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 31, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document defines new mobility options to enable authentication between mobility entities. These options can be used in addition to or in lieu of IPsec to authenticate mobility messages as defined in the base Mobile IPv6 specification.

Table of Contents

1. Motivation

The base specification of Mobile IPv6 [RFC3775] mandates IPsec support between MN and HA for authentication. Also, return routability messages passing via the HA (HoT/HoTi) and mobile prefix discovery messages must be protected using IPsec.

While IPsec (ESP) may offer strong protection (depending on the algorithms used), use of IPsec may not be required/feasible in all cases where Mobile IPv6 may be used. For small handheld devices, the use of IPsec may be too taxing on battery and processor performance. Also depending on the model of home agent deployment (HA deployed by enterprise/service provider), MN may have to VPN back into the enterprise (which may impose dual IPsec requirement on MN).

Moreover, IPsec/IKE based Mobile IPv6 over public wireless carrier's networks may pose serious capacity and scalability challenge. The multiple round trips to perform ISAKMP/IKE to establish IPsec SA may be too taxing on the wireless link, not to mention increase in setup latency during initial access and during handoffs. The use of manual IPsec SA in these large public network deployments suffer from scalability issue and involve provisioning nightmare.

Also, having an authentication mechanism tied to the Mobile's home IP address does not permit the mobility entity to derive or acquire a dynamic home address based on the configured prefix. If the MN's home address is dynamically configured based on a fixed prefix or acquired during network access authentication (PPP, 802.1x etc.), IPsec will most likely not work as the IPsec SAs are tied to the address. The mechanism described in this draft is not tied with mobility entities home IP address and therefore does not mandate SA relationship with an IP address.

Another important motivation for this proposed mechanism is to allow the MN to register with a Home Agent on a dynamically discovered Home

Link. This sort of Dynamic Home Link assignments will allow the operators to leverage the true benefit of dynamic Home Agent assignment. For example the operator may assign a Home Link or Home Agent for the user that is closest to the subnet of attachment of the user. There may be various other reasons for opportunistic Home Agent assignment. The mechanisms described in the draft allows the MN to register with any Home Agent in the home network as long as the MN user shares security association with an entity in the home network such as a AAA server.

2. Overview

This document presents a lightweight mechanism to authenticate the MN at the HA or at the Home AAA based on a shared security association between the MN and the respective authenticating entity.

This document introduces new mobility options to aid in authentication of the MN to the HA or AAA server. The confidentiality protection of the Mobile Prefix Discovery (MPD) and Return Routability (Home KeyGen token) messages is outside the scope of this document.

3. Terminology

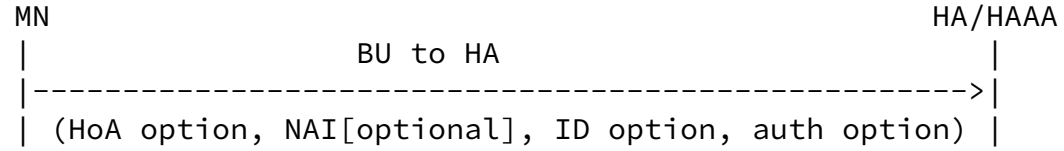
The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

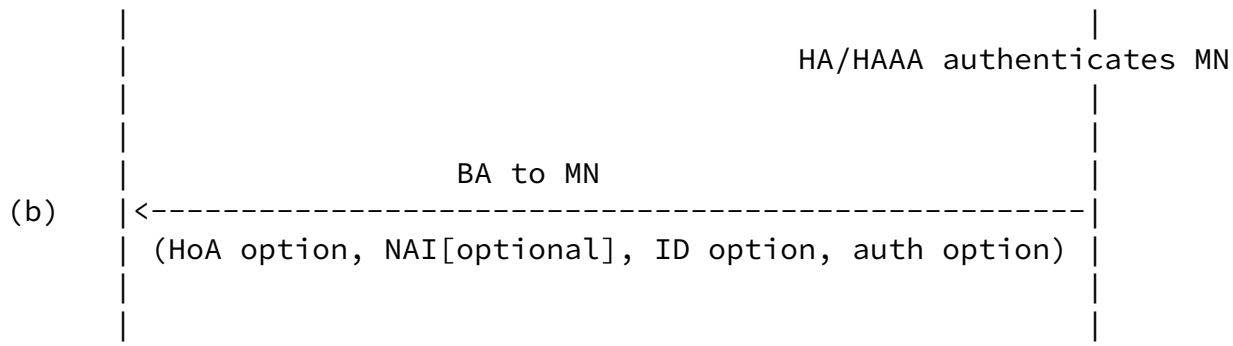
4. General Terms

MN	Mobile Node
HA	Home Agent
SA	Security Association
IPsec	IP Security protocol
ESP	Encapsulating security protocol
BU	Binding Update

BA	Binding Acknowledgement
SPI	Security Parameter Index
MH	Mobility Header
HAAA	Home Authentication Authorization Accounting server
CHAP	CHallenge Authentication Protocol
HoA	Home Address
AVP	Attribute Value Pair
AAA	Authentication Authorization Accounting
NAI	Network Address Identifier

5. Operational flow

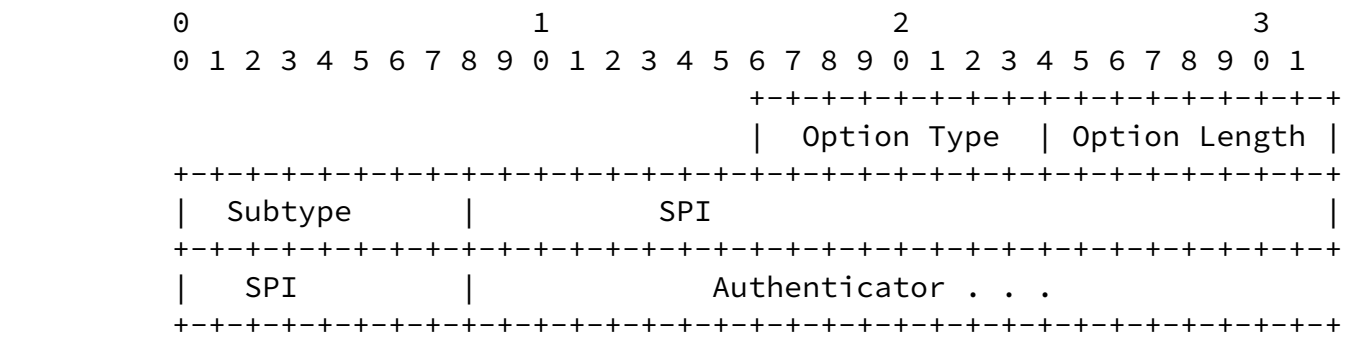




MN may use NAI option as defined in [NAI] to identify itself to the HA while authenticating with the HA. The MN SHOULD use NAI option [NAI] while authenticating with the AAA infrastructure.

6. Mobility message authentication option

This section defines the message authentication mobility option that may be used to secure Binding Update and Binding Acknowledgement messages. This extension can be used along with IPsec or preferably as an alternate mechanism to authenticate binding update and binding acknowledgement messages in 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. It is expected that other subtypes will be defined by other documents in the future.



Option Type:

AUTH-OPTION-TYPE to be 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 sub-type, SPI and authenticator, not including the Option Type and Option Length fields.

Subtype:

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

SPI:

Used to identify the particular security association to use to authenticate the message.

Authenticator:

This field has the information to authenticate the relevant mobility entity. This protects the message beginning at the

Mobility Header upto and including the SPI field.

Alignment requirements :

MUST be aligned on an 8-octet boundary.

6.1 MN-HA authentication mobility option

The format of the MN-HA authentication mobility option is as defined in section 6. This option uses the subtype value of 1. The MN-HA authentication mobility option is used to authenticate the binding update and binding acknowledgement messages based on the shared security association between the MN and the HA.

This must be the last option in a message with mobility header. The authenticator is calculated on the message starting from the mobility header till the SPI value of this option.

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

Mobility Data = care-of address | home address | MH Data

MH Data is the content of the Mobility Header till the SPI field of this extension.

The first 96 bits from the MAC result are used as the Authenticator field.

6.2 MN-AAA authentication mobility option

The format of the MN-AAA authentication mobility option is as defined in section 6. This option uses the subtype value of 2. The MN-AAA authentication mobility option is used to authenticate the binding update and binding acknowledgement messages based on the shared security association between MN and HAAA.

This must be the last option in a message with mobility header. The authenticator is calculated on the message starting from the mobility header till the SPI value of this option.

The MN SHOULD use NAI option [NAI] to enable the Home Agent to make use of available AAA infrastructure which requires NAI.

The MN MUST use either CHAP_SPI or HMAC_CHAP_SPI as defined in [3012bis] to indicate CHAP style authentication. The authenticator shall be calculated as follows:

Authenticator = First (96, HMAC_SHA1 (MN-AAA Shared key, MAC_Mobility Data))).

SPI = CHAP_SPI:

MAC_Mobility Data = MD5 (care-of address | home address | MH Data).

SPI = HMAC_CHAP_SPI:

MAC_Mobility Data = HMAC_MD5 (care-of address | home address | MH Data).

6.2.1 Processing considerations

The MN-AAA authentication mobility option MUST be verified by the AAA infrastructure that has the shared secret with the MN. The HA relays the authenticating information to the HAAA. The HA relies on the HAAA to admit or reject the home registration request from the MN.

6.2.1.1 Home Agent Considerations

Upon receiving a BU from the MN the HA SHALL extract the MN-AAA authenticator and the SPI from the MN-AAA authentication mobility option and extract the NAI from the NAI option [NAI]. The HA SHALL include the extracted MN-AAA authenticator, SPI and the NAI in AAA specific AVPs while initiating the authentication procedure via AAA infrastructure.

7. Mobility message identification option

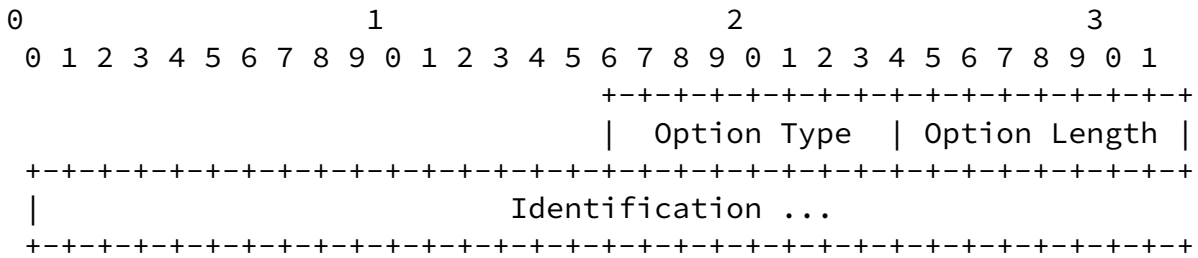
The identification option is used to prevent replay protection. The Identification field carries timestamp for replay protection. This option can be used in binding update and binding acknowledgement messages.

The default method for this purpose is the timestamp method; some other methods may be utilized as well. If the MN uses 'timestamp' as a measure against replay protection, it SHOULD insert the current time of day. When the destination node receives the Binding Update, it will make sure that the 'timestamp' (as included by the sender) is close enough to its own time of the day. A default value of 500 milliseconds MAY be used as a reasonable offset (the time difference between the sender and the receiver).

The low-order 32 bits of the identification option represents fractional seconds, the rest of the bits SHOULD be generated from a good source of randomness.

For the identification field to be valid, the 'timestamp' contained in the Identification field MUST be close enough (as determined by the system implementers) and greater than the HA's and/or HAAA's time of day clock.

The style of replay protection in effect between a mobile node and the HA and/or the HAAA is part of the mobile security association. A mobile node and the HA and/or the HAAA MUST agree on which method of replay protection will be used.



Option Type:

IDENT-OPTION-TYPE to be 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 Identification field.

Identification:

The Identification field carries timestamp for replay protection.

Alignment requirements :

MUST be aligned on an 8-octet boundary.

7.1 Processing considerations

The Identification field is used to let the HA and/or the HAAA verify that a Binding Update message has been generated recently by the MN, and it is not replayed by an attacker from some older registrations.

7.1.1 Home Agent Considerations

The HA processes this option only when MN-HA authentication mobility

option is used in the BU. In this case:

After successful authentication of Binding Update, the Home Agent must verify that the Identification field falls within the replay protection window. If Identification field is not within this window but the authentication of the BU succeeds, HA MUST send a Binding Acknowledgement with error code "TBD by IANA" MIPV6-ID-MISMATCH. In this case, HA must include the correct identification field in the Binding Acknowledgement message.

MN-HA Timestamp: If timestamp based replay check is successful and the authentication succeeds, the HA MUST include the received Identification value in the corresponding field of the Mobility message identification option in the BA.

7.1.2 Mobile Node Considerations

The MN MUST process the Mobility message identification option.

MN-HA Timestamp and MN-AAA Timestamp: The MN MUST set the Identification value in the Mobility message identification option in the BU message according to its own clock. If the MN receives a Binding Acknowledgement with the code MIPV6-ID-MISMATCH, MN must adjust its timestamp and send subsequent Binding Update using the updated value.

7.1.3 AAA server Considerations

The HAAA processes this option only when MN-AAA authentication mobility option is used in the BU. In this case:

After successful authentication of MN's credentials contained in the AVPs, the Home AAA server MUST verify that the Identification field falls within the replay protection window. If Identification field is not within this window, HAAA MUST reject the authentication and authorization request. Upon receiving the reject message from HAAA server, the HA MUST send a Binding Acknowledgement with error code "TBD by IANA" MIPV6-ID-MISMATCH. In this case, HA must include the correct identification field in the Mobility message identification option in the Binding Acknowledgement message.

MN-AAA Timestamp: If timestamp based replay check is successful and the authentication and authorization succeeds, the HAAA does not include any updated Identification value in the accept message. In this case, the HA copies the Identification value from the BU into the corresponding field in the BA. If the replay check fails but authentication succeeds, in the reject message the HAAA MUST include the latest timestamp according to it's own clock.

8. Security Considerations

This document proposes new authentication options to authenticate the control message between MN, HA and/or HAAA (as an alternative to IPsec). The new options provide for authentication of Binding Update and Binding Acknowledgement messages

9. IANA Considerations

The option types AUTH-OPTION-TYPE, IDENT-OPTION-TYPE, as defined in section 6 and 7 respectively are new mobility options. The MIPV6-ID-MISMATCH error code also needs to be defined. IANA should record values for these new mobility options and the new error code.

10. Acknowledgements

TBD.

11 Normative References

[3012bis] Perkins et. al., C., "Mobile IPv4 Challenge/Response Extensions (revised)", draft-ietf-mip4-rfc3012bis-01 (work in progress), April 2004.

[NAI] Patel et. al., A., "Network Access Identifier Option for Mobile IPv6", draft-ietf-mipv6-nai-option-00.txt (work in progress), February 2004.

[RFC2486] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC 2486, January 1999.

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

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@nortelnetworks.com

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

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

Kuntal Chowdhury
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US

Phone: +1 972 685 7788
EMail: chowdury@nortelnetworks.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE

INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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