Network Working Group
Internet-Draft
Expires: November 22, 2004

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

May 24, 2004

Authentication Protocol for Mobile IPv6
draft-patel-mipv6-auth-protocol-01.txt

Status of this Memo

Copyright Notice

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 [BASE] 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).

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.

As per the specification in the current MIPv6 draft [BASE], the return routability messages are protected by IPsec between MN and HA. Specifically, the Home KeyGen token sent by the CN to the MN (via) HA needs to be protected to secure the messages from an eves-dropper on the path between MN and HA. The extensions in this draft encrypts the Home KeyGen token from the HA to MN (based on a shared secret that is either derived, distributed or preconfigured between the MN and the HA). Thus, the integrity of the HoT message is preserved.

This document introduces new mobility options to aid in authentication of the MN and to protect the integrity and confidentiality of return routability and mobile prefix solicitation and advertisement messages.

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
CN	Correspondent Node
IPsec	IP Security protocol
ESP	Encapsulating security protocol
BU	Binding Update
BA	Binding Acknowledgement
HoT	Home Test Message (part of Return Routability test)
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
AES	Advanced Encryption Standard
IV	Initialization Vector

5. Operational flow

```
         MN                                                 HA/HAAA
         |                  BU to HA                           |
   (a)   |---------------------------------------------------->|
         | (HoA option, NAI[optional], ID option, auth option) |
         |                                                     |
         |                                     HA/HAAA authenticates MN
         |                                                     |
         |                                                     |
         |                  BA to MN                           |
   (b)   |<----------------------------------------------------|
         | (HoA option, NAI[optional], ID option, auth option) |
         |                                                     |
         |                                                     |
```

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.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                   |  Option Type  | Option Length |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Subtype      |          SPI                                  |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   SPI         |             Authenticator . . .
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 :

TBD.

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).

Nonces: TBD

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 either timestamps or nonces for replay protection (support for timestamps is mandatory). 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.

```
      0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                       |  Option Type  | Option Length |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                          Identification ...
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 either timestamps or nonces for replay protection (support for timestamps is mandatory).

Alignment requirements :

TBD.

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:

MN-HA Timestamps: 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, 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.

Nonces: TBD

7.1.2 Mobile Node Considerations

Timestamps: If 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.

Nonces: TBD

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:

MN-AAA Timestamps: 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. In the reject message the HAAA MUST include the latest timestamp. 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 Binding Acknowledgement message

Nonces: TBD

8. Encrypted Home KeyGen Token Option

This option is inserted by the HA in the HoT message if MN and HA are using the authentication option defined in this document. If IPsec is used as per [BASE], this processing does not apply.

HA must use the Home KeyGen token from the HoT message and encrypt it as described below. The encrypted token is included in the HoT message. HA must set the Home KeyGen token in the HoT message to zero.

Encrypting the Home KeyGen token provides similar level of security as provided by using IPsec for protecting the HoT messages. The Home KeyGen Token is encrypted using AES [AES].

```
      0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                                       |  Option Type  | Option Length |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                              SPI                              |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                             Nonce                             |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                               |
       |                                                               |
       |                               IV                              |
       |                                                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                           Payload Data . . .
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Option Type:

KEYGEN-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 SPI, Nonce, IV and the payload data fields, not including the Option Type and Option Length field.

SPI:

The SPI corresponds to the SPI of the security associations between MN and HA. It is used to associate the right shared key to decrypt the Home KeyGen token.

Nonce:

The Nonce field is 4 octets in length and is used to ensure the uniqueness of the encryption key used to encrypt each instance of the Home KeyGen Token option occurring in a given HoT message. The contents of each Nonce field in a given HoT message MUST be unique.

IV:

The Initialization Vector (IV) field is 16 octets in length. This value is required to encrypt the first block of plaintext data.

Payload data:

AES (Home KeyGen Token).

Alignment requirements:

TBD.

8.1 Processing Considerations

8.1.1 Home Agent Considerations

Home Agent must intercept the HoT message and if IPsec is not in use between MN and HA as described in [BASE] (for authentication/ encryption of control messages), MUST encrypt the Home KeyGen token as described in section 8.

8.1.2 Mobile Node Considerations

When MN receives a HoT message, if IPsec is not in use between MN and HA, MN must extract the Home KeyGen Token by decrypting the payload data field with the IV, Nonce and the key.

9. Securing The Mobile Prefix Solicitation and Mobile Prefix Advertisement messages

The [BASE] allows the MN to solicit home prefix from the HA. This solicitation message SHOULD be authenticated at the HA before the HA gives out home prefix details to the MN. In order to authenticate the message The MN-HA authentication mobility option SHALL be used. If IPsec is used as per [BASE], this processing does not apply.

In response to the prefix solicitation message, the HA sends Prefix Advertisement Message back the MN. These prefixes SHOULD be encrypted to protect the network from attacks. The prefixes [RFC2461], section 4.6.2 SHOULD be encrypted using a suitable encryption method such as AES [AES]. Encrypting the prefixes provides similar level of security as provided by IPsec using ESP.

9.1 Prefix Encryption Option

to send encrypted prefixes the HA MUST use the following destination option:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     | Prefix Length |L|A| Reserved1 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Preferred Lifetime                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Reserved2                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            SPI                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Nonce                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                                                               |
|                             IV                                |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       payload data  ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type:

PREFIX-OPTION-TYPE to be defined by IANA. An 8-bit identifier of the type mobility option.

Length, Prefix Length, L and A-bit, Reserved1, Valid Lifetime, Preferred Lifetime, Reserved2 are as defined in [RFC2461], section 4.6.2.

SPI:

The SPI corresponds to the SPI of the security associations between MN and HA. It is used to associate the right shared key to decrypt the Encrypted Prefix.

Nonce:

The Nonce field is 4 octets in length and is used to ensure the uniqueness of the encryption key used to encrypt each instance of the prefix encryption option occurring in a given prefix advertisement message. The contents of each Nonce field in a given prefix advertisement message MUST be unique.

IV:

The Initialization Vector (IV) field is 16 octets in length. This value is required to encrypt the first block of plaintext data.

Payload data:

AES (Prefix).

Alignment requirements:

TBD.

9.1.1 Processing Considerations

9.1.1.1 Home Agent Considerations

Upon receiving the Mobile Prefix Solicitation message from a MN, the HA SHOULD authenticate the MN using the MN-HA authentication mobility option that is included in the message. The processing consideration for the MN-HA authentication mobility option is as described in section 6.1.

While sending the Mobile Prefix Advertisement message back to the MN

in response to a solicitation or unsolicited but unicast way, the HA SHOULD encrypt the prefix with a shared secret that is either derived or provisioned between the HA and the MN and use IV and nonce. The encrypted data should be included in the payload data field of the prefix encryption option defined in 9.1. The IV and the nonce used by the HA MUST be included in the respective fields in the prefix encryption option. The HA SHOULD encrypt the prefix using the shared secret, IV and Nonce and the AES mode as indexed by SPI.

9.1.1.2 Mobile Node Considerations

While sending a Mobile Prefix Solicitation message the MN SHOULD include the MN-HA authentication mobility option. The calculation of the authenticator can be performed as:

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

Data = All fields in the IP header and the message body.

Upon receiving a Mobile Prefix Advertisement message from the HA in a solicited or unsolicited manner, the MN SHOULD decrypt the prefix using the shared secret, IV and Nonce and the AES mode as indexed by SPI.

10. 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. These do not provide ways for encrypting these messages.

In terms of protecting the return routability messages, this mechanism provides a way to encrypt the Home KeyGen token from CN to MN on the path between HA and MN.

In terms of protecting Prefix Solicitation and Prefix Advertisement messages this specification provides ways to calculate and include message authenticators and provides ways to send encrypted prefixes to the MN.

11. IANA Considerations

The option types AUTH-OPTION-TYPE, IDENT-OPTION-TYPE, KEYGEN-OPTION-TYPE and PREFIX-OPTION-TYPE as defined in section 6, 7 and 8 respectively are new mobility options. MIPV6-ID-MISMATCH error code also needs to be defined. IANA should record values for these new mobility options and the new error code.

12. Acknowledgements

TBD.

13 Normative References

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

[AES] "National Institute of Standards. FIPS Pub 197: Advanced Encryption Standard (AES).", 26 November 2001.

[BASE] Perkins, C., Johnson, D. and J. Arkko, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-24 (work in progress), June 2003.

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

[RFC1700] Reynolds, J. and J. Postel, "Assigned Numbers", RFC 1700, October 1994.

[RFC2461] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

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

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

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

Acknowledgment

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