Network Working Group B. Patil
Internet-Draft Nokia
Intended status: Informational G. Dommety
Expires: May 6, 2009 Cisco
November 2, 2008

Why Authentication Data suboption is needed for MIP6
draft-ietf-mip6-whyauthdataoption-07.txt

Status of this Memo

Abstract

Mobile IPv6 defines a set of signaling messages that enable the mobile node (MN) to authenticate and perform registration with its home agent (HA). These authentication signaling messages between the mobile node and home agent are secured by an IPsec SA that is established between the MN and HA. The MIP6 working group has specified a mechanism to secure the binding update and binding acknowledgement messages using an authentication option, similar to the authentication option in Mobile IPv4, carried within the signaling messages that are exchanged between the MN and HA to establish a binding. This document provides the justifications as to why the authentication option mechanism was needed for Mobile IPv6 deployment in certain environments.

Table of Contents

1. 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 [RFC2119].

2. Introduction

Mobile IPv6 relies on the IPsec Security Association between the Mobile Node (MN) and the Home Agent (HA) for authentication of the MN to its HA before a binding cache can be created at the HA. An alternate mechanism that does not rely on the existence of the IPsec SA between the MN and HA for authenticating the MN is needed in certain deployment environments. This document captures the reasons that were outlined, and explains why such a mechanism was considered essential to ensure the applicability of MIP6 as a protocol for wider deployment. It was noted that the alternate solution does not imply that the IPsec based solution would be deprecated. It simply meant that in certain deployment scenarios there was a need for supporting MIP6 without an IPsec SA between the MN and HA. So the alternate solution would be in addition to the IPsec based mechanism specified in the base RFCs, RFC 3775 [RFC3775], RFC 3776 [RFC3776] and RFC 4877 [RFC4877]. It was noted that some of the challenges of deploying MIP6 in certain types of networks arose from the dependence on IKE which did not integrate will with a AAA backend infrastructure. IKEv2 solves this problem. However at the time of discussion on the need for the authentication protocol, the specification for using Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture [RFC4877] was still work in progress and as a result an alternative solution needed. This document is intended to capture for archival purposes the reasoning behind the need for the authentication protocol which is specified in [RFC4285]. It should be noted that some of the arguments for justifying the specification of the authentication protocol have been made redundant as a result of the specification of Mobile IPv6 operation with IKEv2 [RFC4877]. However some of the arguments discussed in this document are still applicable and justify usage of the authentication protocol in certain deployment environments.

3. Background

Mobile IPv6 signaling involves several messages. These include:

- The Binding update/Binding ACK between the mobile node and the home agent.

- The route optimization signaling messages which include HoTI/Hot, CoTI/CoT and BU/BAck between the MN and CN. HoTI and HoT signaling messages are routed through the MNs HA.

- Mobile prefix solicitation and advertisements between the MN and HA.

- Home agent discovery by MNs.

The signaling messages between the MN and HA are secured using the IPsec SA that is established between these entities. The exception to this are the messages involved in the home agent discovery process. [RFC4877] specifies the establishment of the IPsec SA using IKEv2.

4. Applicability Statement

The authentication option specified in the Authentication Protocol for MIP6 [RFC4285] provides a solution for MIP6 deployment in environments which an operator may not require IPsec based security for the signaling. The reasons for an operator choosing to deploy MIP6 without mandating IPsec based security for signaling messages between the MN and HA could be many. Some of these are for example:

1. Operators deploying MIP6 in cellular networks may consider IPsec and IKEv2 as adding overhead to the limited bandwidth over the air interface. The overhead here is in terms of the bytes that IPsec and IKEv2 introduce to the signaling.

2. Operators may consider the number of messages between the MN and HA that are required to establish the IPsec SA as too many. The number of transactions chew into the capacity of limited bandwidth air interfaces when MIP6 is used in such environments. It also adds additional latency to the establishment of the binding.

3. In many deployments the authentication credentials already exist in a AAA server. These credentials are used for authenticating a user and authorizing network access. The same credentials and security parameters can be reused for MIP6 security as well.

4. Dynamic assignment of home agents is needed in certain deployments to minmize the latency of the backhaul. This is done by allocating an HA in a visited network for example. Requiring IPsec SAs with home agents that are dynamically assigned is an overhead especially when the HA is in a visited network.

5. Signaling messages between the MN and HA may be in certain deployments over secure link-layers. The lower layers provide ciphering and security for the messages and hence the need for IPsec to do the same for MIP6 messages does not exist.

One such example of networks that have such characteristics are cdma networks as defined in the 3GPP2 X.S0011-002-D [3GPP2 X.S0011-002-D] specification. Mobile WiMAX (Worldwide interoperability for Microwave Access) which is based on IEEE 802.16e also specifies in the network architecture the use of MIP6, with the default security for signaling being the authentication protocol (RFC4285). The WiMAX network architecture specifications are available at: [WiMAX-NWG].

5. Justification for the use of the authentication option

The following two sections provide the reasoning for standardizing the authentication option based registration process for Mobile IPv6. Section 5.1 provides the key arguments for the use of authentication option. Section 5.2 provides further explanation and additional motivations for the authentication option.

5.1. Motivation for use of authentication option in cdma2000 wireless networks

cdma2000 networks deployed and operational today use Mobile IPv4 for IP mobility. Operators have gained a significant amount of operational experience in the process of deploying and operating these networks. 3GPP2 has specified Mobile IPv6 in Revision D of the 3GPP2 X.S0011-002-D [3GPP2 X.S0011-002-D] specification (which specifies the packet data architecture). The following are the deployment constraints that existing CDMA networks have to deal with when deploying Mobility service based on IPv6:

- o Operators intend to leverage the Mobile IPv4 deployment and operational experience by ensuring that Mobile IPv6 has a similar deployment and operating model.

- o Operators will have two parallel networks, one that offers IPv4 mobility with MIP4 and another providing IPv6 mobility using MIP6.

- o The same backend subscriber profile database, security keys etc. are intended to be used for both Mobile IPv4 and, Mobile IPv6 service. However from a security standpoint, the reuse of the same keys with multiple algorithms/protocols is a bad idea.

- o The same user configuration information, i.e the identity and keys associated with a user will be used for IP mobility service in IPv4 and/or IPv6 networks. The only security association that is preconfigured is a shared secret between the mobile node and the home-AAA server. This was in contrast with an earlier version of the Mobile IPv6 model which required an IPsec SA between the MN and HA. At the time of this writing the IKEV2 based solution for establishing an IPsec SA [RFC4877] was not available. IKEv2 does enable integration with a a AAA backend.

- o At the time of specifying the authentication protocol, the Mobile IPv6 specification did not support the dynamic assignment of home agent and home address. However work done in the MIP6 working group on bootstrapping of Mobile IPv6 as specified in [RFC5026] and MIP6-bootstrapping for the Integrated Scenario [I-D.ietf-mip6-bootstrapping-integrated-dhc] addresses this

deficiency. The mechanism defined in Authentication protocol for Mobile IPv6 [RFC4285] is capable of handling authentication even in the case of dynamic assignments (and is similar to what is used in current MIPv4 deployments).

Consequently, MIP6 as specified at the time the authentication protocol was being specifid did not satisfy many of the deployment requirements. The Authentication protocol for MIP6 [RFC4285] along with the MN Identifier option for MIP6 [RFC4283] are enabling the deployment of Mobile IPv6 in a manner that is similar to what is deployed in cdma2000 networks today. This authentication model is very similar to the one adopted by the MIPv4 WG. This is explained in detail in the 3GPP2 X.S0011-002-D [3GPP2 X.S0011-002-D] specification.

The earlier MIP6 deployment model which requires an IPsec SA which is either configured manually or established using IKE does not have synergy with the deployment models of 3GPP2 or WiMAX networks. This issue has however been alleviated with the publication of RFC4877 which enables the establishment of an IPsec SA using IKEv2 and is also able to integrate with the backend AAA infrastrucuture that is responsible for the authentication of the MN in 3GPP2 and WiMAX networks.

5.2. Additional arguments for the use of Authentication option

The use of IPsec for performing Registration with a home agent is not always an optimal solution. While it is true that IPsec is an integral part of the IPv6 stack, it is still a considerable overhead from a deployment perspective of using IPsec as the security mechanism for the signaling messages between the MN and HA. This statement is a result of experience gained from deployment of Mobile IPv4. MIP4 does not rely on IPsec for securing the Registration signaling messages.

Deployment of Mobile IPv6 on a large scale is possible only when the protocol is flexible for being adapted to various scenarios. The scenario being considered is the deployment in cdma2000 net- works or WiMAX networks. cdma2000 networks are currently deployed in many countries today and WiMAX deployments are beginning. The packet data network architecture of cdma2000 [3GPP2 X.S0011-002-D] includes a MIP4 foreign agent/Home agent and a Radius based AAA infrastrucutre for authentication, authorization and accounting purposes. The AAA infrastructure provides the authentication capability in the case of Mobile IPv4.

Typically, the Mobile Node shares a security association with the AAA-Home entity. This is the preferred mode of operation over having

a shared secret between the MN and HA because the AAA-Home entity provides a central location for provisioning and administering the shared secrets for a large number of mobiles (millions). This mode of operation also makes dynamic home address and dynamic home agent assignment easier. A similar approach is needed for the deployment of Mobile IPv6 in these networks. There is no practical mechanism to use IPsec directly with the AAA infrastructure with out the use of IKE or some other mechanism that enables the establishment of the IPsec SA between the MN and HA.

Mobile IPv6 as specified in RFC3775 and RFC3776 is based on a very specific model for deployment. It anticipates the Mobile nodes having a static home IPv6 address and a designated home agent. This is not practical in most deployment scenarios being considered. An IPsec SA is expected to be created, either via manual keying or established dynamically by using IKE or IKEv2. These assumptions do not necessarily fit in very well for the deployment model envisioned in cdma2000 or WiMAX networks. These limitations have however been overcome as a result of the bootstrapping specifications as per [RFC5026] and MIP6-bootstrapping for the Integrated Scenario [I-D.ietf-mip6-bootstrapping-integrated-dhc]

cdma2000 and WiMAX networks would prefer to allocate home addresses to MNs on a dynamic basis. The advantage of doing so is the fact that the HA can be assigned on a link that is close to the MNs point of attachment. While route-optimization negates the benefit of having a home-agent on a link close to the MN, it cannot be always guaranteed that the MN and CN will use or support route optimization. There may also be instances where the operator prefers to not allow route optimization for various reasons such as accounting aggregation or enforcing service contracts. In such cases an HA that is close to the MNs point of attachment reduces the issues of latency etc. of forward and reverse tunnelling of packets between the MN and HA.

cdma2000 networks that are operational today have large numbers of subscribers who are authenticated via the AAA infrastrucure. Deployment of Mobile IPv6 should leverage the existing AAA infrastructure. The security model needed in these networks is an SA between the MN and AAA-Home entity. This is the primary security association that should be used for authenticating and authorizing users to utilize MIPv6 service. This SA is then used for establishing session keys between the MN and the dynamically assigned HA for authenticating subsequent binding updates and binding acknowledgements between them. Establishing an IPsec SA between the MN and HA using AAA infrastrucure was not specified for Mobile IPv6 at the time the Authentication protocol was being specified. RFC3776 explains how IKE is used for establishing the SA between the MN and HA. [RFC4877] has been published subsequently and hence the issue of

establishing an IPsec SA dynamically between the MN and HA no longer exists. cdma2000 network operators would prefer to assign home addresses to the MN on a dynamic basis and do this preferably using the AAA infrastrucutre which contains subscriber profile and capability information. This was not possible prior to the specification of the bootstrapping mechanism in [RFC5026].

A large subset of MNs in cdma2000 networks do not have IKE capability. As a result the use of RFC3776 for setting up the MN-HA IPsec SA is not an option. It should also be noted that IKE requires several transactions before it is able to establish the IPsec SA. [RFC4877] specifies the establishment of an IPsec SA between the MN and HA using IKEv2. It is possible that not all MNs in a deployment will support IKEv2 and hence an alternative mechanism provides the needed flexibility.

cdma2000 network operators are extremely conscious in terms of the number of messages sent and received over the air-interface for signaling. The overhead associated with sending/receiving a large number of signaling messages over the air interface has a direct impact on the overall capacity and cost for the operator. Optimization of the number of messages needed for using a service like Mobile IPv6 is of great concern. As a result the use of IKE for Mobile IPv6 deployment is considered as being suboptimal in certain network architectures and deployment scenarios from the perspective of message overhead.

Another downside of IKE for setting up the IPsec SA between the MN and HA is that IKE does not integrate very well with the Radius based AAA back-end. Since operators rely on the AAA infrastrucure to provision subscribers as well as define profiles, keys etc. in the AAA-Home, there is no getting away from the use of AAA in cdma2000 networks. IKEv2 does address this problem. However from a timeline perspective the availability of IKEv2 specifications for Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture [RFC4877] and implementations did not meet the need of operators that were relying on 3GPP2 specifications. With the specification of IKEv2 and publication of RFC4877 the integration with AAA backends is no longer an issue.

In summary the model of Mobile IPv6 deployment which mandated the existence of an IPsec SA between the MN and HA, as specified in RFCs 3775 and 3776, was too rigid and did not meet the requirements of operators building networks based on the cdma2000 [3GPP2 X.S0011-002-D] specifications. To address this shortcoming, the authentication protocol [RFC4285] was specified.

6. Application of Mobile IPv6 in CDMA Networks

Sections 6.1 and 6.2 describe the IPv4 based mobility architecture in cdma networks and IPv6 based mobility architecture in cdma Networks respectively. For further details associated with the description below, please refer to Section 5, "MIP6 Operation", in 3GPP2 specification [3GPP2 X.S0011-002-D].

6.1. IPv4 based mobility architecture in cdma2000 networks

The figure below shows a high level view of the key network elements that play a role in providing IP mobility using Mobile IPv4.

```
                 +--------------+           +----------------------+
                 |   +------+   |           |   +------+           |
                 |   |      |   |           |   |      |           |
                 |   |F-AAA |   |           |   |H-AAAH|           |
                 |   |      +-------------------+      |           |
                 |   +---+--+   |           |   +--+---+           |
                 |       |      |           |      |               |
                 |       |      |           |      |               |
      +------+   |   +---+--+   |           |   +--+---+           |
      |      |   |   |      |   |           |   |      |           |
      |  MN  +- -|- -+ PDSN + --  --  --  --  - +  HA  |           |
      |      |   |   |  /FA |   |           |   |      |           |
      +------+   |   +------+   |           |   +------+           |
                 |              |           |                      |
                 +--------------+           +----------------------+
```

Figure 1: cdma2000 packet data network architecture with Mobile IPv4

The cdma mobility architecture based on MIPv4 is explained below. In this architecture, mobility is tightly integrated with the AAA infrastructure. The Mobile is configured with a NAI (Network Access Identifier) and a MN-AAA Key. The MN-AAA key is a shared Key that is shared between the MN and the Home AAA server.

Below is the access link setup procedure:

(1) Bring up PPP on MN/PDSN (access router link). PPP authentication is skipped. Mobile IP Authentication is performed via the FA.

(2) PDSN sends a Mobile IP challenge to the MN on PPP link (RFC 3012).

(3) MN sends a MIP registration request (RRQ), which includes the users NAI, challenge and a MN-AAA extension which has challenge response and a MN-HA extension which is generated based on the MN-HA key.

(4) PDSN extracts the MIP NAI/Challenge and response from MIP MN-AAA extension sends an Access Request to F-AAA (challenge/response using MD5).

(5) F-AAA may forward it to H-AAA if needed (based on realm).

(6) AAA authenticates the chap-challenge/response and returns "success" if authentication succeeds.

(7) PDSN forwards Registration Request (RRQ) to HA.

(8) HA authenticates the RRQ (MHAE extension). HA may optionally authenticate with AAA infrastructure (just like PDSN as in #4).

(9) If authentication is successful, HA creates a binding and sends a success Registration Reply (RRP) to PDSN.

(10) PDSN creates a visitor entry and forwards the RRP to MN.

6.2. IPv6 based mobility architecture in cdma2000 networks

Due to the need for co-existence with MIPv4, and having the same operational model, the 3GPP2 standards body is adopting the following mobility architecture for MIPv6.

```
                        Access Domain                  Home Domain
                  +--------------+           +----------------------+
                  |   +------+   |           |   +------+           |
                  |   |      |   |           |   |      |           |
                  |   |F-AAA |   |           |   |H-AAA |           |
                  |   |      +-------------------+      |           |
                  |   +---+--+   |           |   +--+---+           |
                  |       |      |           |      |               |
                  |       |      |           |      |               |
       +------+   |   +---+--+   |           |   +--+---+           |
       |      |   |   |      |   |           |   |      |           |
       |  MN  +- -|- -+ PDSN + --  --  --   --  - +  HA  |           |
       |      |   |   |  /AR |   |           |   |      |           |
       +------+   |   +------+   |           |   +------+           |
                  |              |           |                      |
                  +--------------+           +----------------------+
```

Figure 2: cdma2000 packet data network architecture with Mobile IPv6

The Mobile is configured with an NAI (Network Access Identifier) and a MN-AAA Key. The MN-AAA key is a shared Key between the MN and the Home AAA server.

6.2.1. Overview of the mobility operation in IPv6 based cdma2000 networks

The following steps explain at a very generic level the operation of IP mobility in cdma2000 networks:

(1) The MN performs Link Layer establishment. This includes setting up the PPP link. PPP-Chap authentication is performed. This is authenticated by the PDSN/AR by sending an Access Request to the F-AAA (and to the H-AAA when/if needed). Optionally, the MN acquires bootstrap information from the Home Network (via the PDSN; PDSN receives this information in Access Accept). The bootstrap information includes Home address and Home agent assignment. The MN uses stateless DHCPv6 [RFC3736] to obtain the bootstrap information from the PDSN.

(2) The MN begins to use the HoA that was assigned in step 1. If no HoA was assigned at step 1, the MN generates (auto-configures) an IPv6 global unicast address based on the prefix information received at step 1.

(3) At this step the MN sends a Binding Update to the selected Home Agent. In the BU, the MN includes the NAI option, timestamp option and MN-AAA auth option.

(4) The HA extracts the NAI, authenticator etc. from the BU and sends an access request to the Home RADIUS server.

(5) The Home RADIUS server authenticates and authorizes the user and sends back a RADIUS Access-Accept to the HA indicating successful authentication and authorization.

(6) At this step the HA performs a replay check with the ID field in the received BU. The HA also performs proxy Duplicate Address Detection (DAD) on the MN's home address (global) using proxy Neighbor Solicitation as specified in RFC 2461.

(7) Assuming that proxy DAD is successful, the HA sends back a Binding Acknowledgment to the MN. In this BA message the HA includes the MN-HA mobility option, NAI mobility option and the ID mobility option.

6.2.2. Authentication and Security details

Access Link Setup, Access Authentication and Bootstrapping:

(1) MN brings up PPP session. PDSN triggers the MN to perform CHAP authentication, as part of access authentication, while bringing up PPP link.

(2) The MN is authenticated using PPP-CHAP by the H-AAA (Home AAA), via the F-AAA (Foreign AAA).

(3) H-AAA may optionally send HoA and HA IP address to the PDSN for bootstrapping the MN (skipping details).

Mobile IPv6 Authentication:

The Call Flow for the initial authentication (the number in the parenthesis corresponds to the explanation below)

```
 MN                                    HA                    H-AAA
  |              BU to HA (4)           | RADIUS Access-ReQ(5)
  |------------------------------------>|-------------------->|(6)
  | (includes NAI option, MN-ID option, |                     |
  | Mesg ID option, MN-AAA Auth Option) |RADIUS Access-Accept|(7)
  |
                                        |<-------------------|
  |                                     |                    |
  |                             HA/AAAH authenticates MN
  |
  |                                     |(8)
  |
  |                                     |
  |
  |              BA to MN    (9)        |
  |
  |<------------------------------------|--------------------|
  | (including MN-ID option,            | (10)
  |  Message ID option,                 |
  |  MN-HA auth options)                |                    |
```

Figure 3: Flow diagram for initial authentication

(4) MN sends Binding Update (BU) to the HA. Binding Update is authenticated using MN-AAA option. The authenticator in MN-AAA option is calculated using hash of BU and MN-AAA shared key. It uses HMAC_SHA1 algorithm. The SPI field in MN-AAA is set to 3 (defined in the draft) BU also includes NAI and timestamp among other details. The hash of BU includes the 'timestamp' option and thus provides proof of liveness to prevent replay.

(5) HA on receiving the BU, extracts the NAI, timestamp, authenticator from MN-AAA option and generates hash of BU. HA sends an Access Request to the AAA and puts this information in 3gpp2 defined VSAs (Vendor Specific Attributes). The NAI is put in username in Access Request. The other attributes sent are: timestamp option, hash of the BU (till SPI field of MN-AAA auth option) and the authentication data from MN-AAA auth option.

(6) AAA (Radius server which interprets these attributes), authenticates the MN based on the hash of BU and authenticator. Proceed to step 7

(7) AAA calculates a session key based on MN-AAA shared secret and timestamp and sends this to HA in Access-Accept (in a 3gpp2 defined VSA).

(8) (skipping details for timestamp processing at HA) HA creates a binding and a security association per Authentication Protocol for MIP6 [RFC4285]. The key for this association is retrieved from Access Accept and is referred to as session key. HA associates a fixed SPI of 5 with this SA and is associated with the binding for the MN

(9) HA sends a Binding Acknowledgement (BA) to the MN. BA has the MN-HA authentication option, authenticated using the session key. This option has the SPI set to 5.

(10) On receiving a BA, MN calculates the session-key (using same method as AAA) and associates it with SPI value of 5.

MN derives the session key and SA using the timestamp in the BU that the MN sent and the MN-AAA shared key. The MN uses this key to authenticate the MN-HA option in Binding Ack. If authentication is successful, MN creates a security association with SPI=5. This key is used to authenticate further BU to the HA using the MN-HA auth option. Once the binding lifetime expires and binding is deleted, the binding as well as the security association based on the Integrity Key is removed at the MN and HA.

Migration from MobileIPv4 to MobileIPv6 utilizes the same network

architecture and specially the same AAA infrastructure. Thus, it is natural to have similar signaling in MIP6 as in MIP4, specifically the authentication with AAA infrastructure.

7. Limitations of the Authentication Protocol option

While the authentication protocol as specified in [RFC4285] provides Mobile IPv6 [RFC3775] deployments a certain degree of flexibility it does have a few disadvantages as well. These are:

(1) The route optimization feature specified in RFC3775 requires a secure transport (IPsec/ESP mode) between the MN and HA. In cases where the authentication protocol (RFC4285) is used as the means for securing the MIP6 signaling between the MN and HA, route optimization should be switched off unless the security of the signaling between the MN and HA can be guaranteed via other means (such as link layer security in the case of 3GPP2 networks).

(2) The MIP6 protocol is responsible for the security of the signaling messages as opposed to relying on IPsec for providing the security.

(3) In 3GPP2 networks, link-layer security mechanisms, ingress filtering at the PDSN, and various network domain security mechanisms largely ensure that reverse tunnelled packets received by the HA do not have spoofed source addresses, and their contents have not been modified. This implies the HA can determine the specific MN which sent the packet simply by verifying the outer source IP address matches the currently registered care-of address. Authentication of payload packets can be necessary for e.g.:

- Authenticating signalling messages other than BU/BAck between the MN and HA, such as ICMPv6, MLD, and DHCPv6.

- Enforcing access control to the network behind the HA.

- Accounting or other flow-specific processing performed by the HA.

  This means the authentication option is of limited applicability in environments where the HA can received reverse tunneled packets with spoofed source IP addresses and/or modified contents.

(4) As described in [RFC4285], the authentication option assumes that the MN-AAA shared key and security association are created by out-of-band mechanisms. These mechanisms are specific to specific deployment environments. IKEv2, on the other hand, supports a wide range of authentication mechanisms, such as certificates and EAP methods, and is independent of the access

network technology being used. However, it would be possible to specify a similar authentication and key management protocol for the authentication option in the future.

(5) Sending the long-term user identity (NAI) in clear raises privacy concerns. These concerns are addressed by access network and network domain security mechanisms in 3GPP2 networks, but do limit the applicability in networks where sniffing other users' traffic is possible.

(6) RFC 4285 does not specify a mechanism for creating the MN-HA shared key and SA from the MN-AAA SA (unlike similar Mobile IPv4 mechanisms defined in [RFC3957], and thus rely on deployment specific mechanisms not standardized in IETF.

(7) The authentication option does not support negotiation of cryptographic algorithms.

(8) The replay protection mechanisms in [RFC4285] rely on timestamps, and thus requires reasonably synchronized clocks (by default, +/- 7 seconds). This assumes the MN implements, and is configured to use, some mechanism for synchronizing its clock.

8. Security Considerations

When MIP6 signaling messages use IPsec with ESP encapsulation, they are accorded privacy on the links over which the messages traverse. When MIP6 signaling messages are secured using the authentication protocol, such ciphering capability will have to be enabled by the underlying link layers. It should be noted that the MIP6 signaling messages are susceptible to snooping/sniffing when the authentication protocol [RFC4285] is used. Route optimization messages need to be secured between the MN and HA and this is not possible with the authentication protocol. Howver route optimization is not supported in the current specification of the authentication protocol in [RFC4285].

Security issues with RFC4285 are specifically:

1. Key length. This is being addressed in the 4285bis I-D [I-D.ietf-mip6-rfc4285bis] at the present time.

2. The keys used for securing the signaling between the MN and HA are derived from a security association that exists between the MN and AAA. The MIP6 keys which are bootstrapped from the MN-AAA SA are transient. Limiting the lifetime of the keys to shorter periods should be recommended.

3. Location privacy is an issue in the absence of lower layer security in the case of shared links.

9. IANA Considerations

This document has no actions for IANA.

10. Conclusion

Mobile IPv6 has been published as a standards track RFC [RFC3775] in 2004. Deployment of this protocol on a large scale is in the interest of the IETF and the working group as well as that of many people who have worked on this. A rigid model for deployment will cause the protocol to be limited to an academic exercise only. It is extremely critical that the working group consider the needs of the industry and the deployment scenarios and address them accordingly. This document captures the reasoning behind the need for the authentication protocol which has been published as RFC 4285. RFC4877 has alleviated some of the issues that have been of primary concern and motivators for the authentication protocol. However the IETF should consider the architectures of networks such as 3GPP2 and WiMAX and their security models and enable deployment of Mobile IPv6 without requiring IPsec.

11. Acknowledgements

The authors would like to thank Alpesh Patel, AC Mahendra, Kuntal Chowdhury and Vijay Devarapalli for their input and discussions. Jari Arkko has reviewed the ID and provided valuable feedback. Thomas Narten has provided valuable reviews and made significant improvements to the text in this document. In his role as the IETF liaison to 3GPP2, Thomas Narten has ensured that the IETF understands the 3GPP2 requirements. Pasi Eronen in his role as the Security AD has reviewed and helped improve the document. Vidya Narayanan has reviewed the document from a security directorate perspective and provided input that has been incorporated.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997, <ftp://ftp.isi.edu/in-notes/rfc2119>.

[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.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[I-D.ietf-mip6-rfc4285bis] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-rfc4285bis-03 (work in progress), July 2008.

12.2. Informative References

[RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

[RFC5026] Giaretta, G., Kempf, J., and V. Devarapalli, "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC3957] Perkins, C. and P. Calhoun, "Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4", RFC 3957, March 2005.

[I-D.ietf-mip6-bootstrapping-integrated-dhc] Chowdhury, K. and A. Yegin, "MIP6-bootstrapping for the Integrated Scenario",

draft-ietf-mip6-bootstrapping-integrated-dhc-06 (work in progress), April 2008.

[3GPP2 X.S0011-002-D]
"3GPP2 X.S0011-002-D "cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services; http://www.3gpp2.org/Public_html/specs/X.S0011-002-D_v1.0_060301.pdf "", February 2006.

[WiMAX-NWG]
"WiMAX End-to-End Network Systems Architecture http://www.wimaxforum.org/technology/documents/WiMAX_Forum_Network_Architecture_Stage_2-3_Rel_1v1.2.zip", May 2008.

Authors' Addresses

Basavaraj Patil
Nokia
6021 Connection Drive
Irving, TX 75039
USA

Email: basavaraj.patil@nokia.com

Gopal Dommety
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: gdommety@cisco.com

Full Copyright Statement

Intellectual Property