MIP6 Working Group
Internet-Draft
Expires: March 2, 2006
Basavaraj Patil
Nokia
Gopal Dommety
Cisco
August 29, 2005

Why Authentication Data suboption is needed for MIP6
draft-patil-mip6-whyauthdataoption-01

Status of this Memo

Copyright Notice

Abstract

Mobile IPv6 defines a set of 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 ID draft-ietf-mip6-auth- protocol-04.txt specifies a mechanism to secure the binding update and binding acknowledgement messages using an

authentication option, similar to authentication option in Mobile IPv4, carried within the 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 is needed for Mobile IPv6 deployment in certain deployment environments.

Table of Contents

1. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant implementations.

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 outlines some of the reasons why such a mechanism is essential to ensure the applicability of MIP6 as a protocol for wider deployment. It should be noted that the alternate solution does not imply that the IPsec based solution would be deprecated. It simply means that in certain deployment scenarios there is 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] and RFC 3776 [RFC3776]. It should be noted that some of the challenges of deploying MIP6 in certain types of networks arise from the dependence on IKE which does not integrate will with a AAA backend infrastructure. IKEv2 does address this problem. However at the present time the specification for using IKEv2 with MIP6 [I-D.ietf-mip6-ikev2-ipsec] is still work in progress and as a result an alternative solution is necessary.

3. Background

Mobile IPv6 signaling involves several messages. These include:

- o The binding update/Binding ACK between the mobile node and the home agent.
- o 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.
- o Mobile prefix solicitation and advertisements between the MN and HA.
- o 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.

4. Applicability Statement

The Authentication option specified in this document was designed to be used by 3GPP2 based CDMA networks as defined in 3GPP2 X.S0011-D [3GPP2 X.S0011-D]. These networks have all of the following characteristics:

1. Access Networks in which there is a Strong Access Athentication
2. Networks in which there is an out-of-band mechanism to re-fresh the security association between the Mobile Node and HA
3. Networks in which there is exist out-of-band mechanisms to refresh the security association between the Mobile Node and AAA
4. Networks in which there is a requirement to minimize the amount of signalling between the Mobile Node and HA
5. Networks in which the AAA infrastructure is used to authenticate the Mobile Node

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 is now in the process of specifying Mobile IPv6 in Revision D of the 3GPP2 X.S0011-D [3GPP2 X.S0011-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:

- Operators intend to leverage the Mobile IPv4 deployment and operational experience by ensuring that Mobile IPv6 has a similar deployment and operating model.
- 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 mobility services.
- 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 is in contrast with the currently specified Mobile IPv6 model which requires an IPsec SA between the MN and HA. It can be argued that IKEv2 does provide the capability to be integrated with a AAA backend. However IKEv2 is not an option that can be considered because of the deployment timelines of operators relying on 3GPP2 standards.
- o Current Mobile IPv6 specification does not facilitate the dynamic assignment of home agent and home address. In order to allow such dynamic assignments (which are already supported in Mobile IPv4), a new mechanism is needed. The mechanism defined in the auth-option ID [I-D.ietf-mip6-auth-protocol] is capable of handling authentication even in the case of dynamic assignments.
- o The identity of a user in MIP4 based cdma2000 networks is an NAI. Mobile IPv6 as per RFC3775 specifies the IPv6 home address as the identity of the mobile node.

MIP6 as specified today does not satisfy these requirements. The auth-option ID [I-D.ietf-mip6-auth-protocol] along with the Identifier option ID [I-D.ietf-mip6-mn-ident-option] 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-D [3GPP2 X.S0011-D] specification.

Hence, with the current MIP6 specifications and architecture that relies on IPsec as the sole means for securing the signaling between the MN and HA, it is not possible to accomplish a deployment that mirrors that of MIP4 for cdma deployments. Therefore, the MIP6 WG has by consensus developed a solution that can optionally be used to authenticate the MN-HA signaling messages without relying on the existence of the IPsec SA.

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. cdma2000 networks are currently deployed in many countries today. The packet data network architecture of cdma2000 [3GPP2 X.S0011-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 implies a very specific model for deployment. It anticipates the Mobile nodes having a static home IPv6 address and a designated home agent. An IPsec SA is expected to be created, either via manual keying or established dynamically by using IKE. These assumptions do not necessarily fit in very well for the deployment model envisioned in cdma2000 networks.

cdma2000 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 is not specified for Mobile IPv6 today. RFC3776 explains how IKE is used for establishing the SA between the MN and HA. And even in this case, the MN has a designated home address. 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.

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.

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 detrimental to the operators bottom line.

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 [I-D.ietf-mip6-ikev2-ipsec] and implementations do not meet the need of operators that are currently relying on 3GPP2 specifications.

In summary the current model of Mobile IPv6 deployment which mandates the existence of an IPsec SA between the MN and HA, as specified in RFCs 3775 and 3776, is too rigid and does not meet the requirements of operators building networks based on the cdma2000 [3GPP2 X.S0011-D] specifications. This is a problem that needs to be addressed in order to ensure wide-scale deployment of the protocol.

6. Solution Proposal

The above issues can be addressed by developing a solution that allows MIPv6 deployment that does not mandate the use of IPsec for

securing the binding update and binding acknowledgment messages between the MN and HA. A solution similar to the one that is used in Mobile IPv4 today can be applied to Mobile IPv6 as well. The experience gained in deploying Mobile IPv4 in cdma2000 networks on a large scale can be reused for Mobile IPv6 also. The only consideration is that the alternative solution should not be vulnerable to attacks that are otherwise prevented by the use of IPsec. Sections 4.1 and 4.2 describe the IPv4 based mobility architecture in cdma networks and IPv6 based mobility architecture in cdma Net- works respectively.

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

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 a very high level overview of IP mobility in cdma2000 networks:

The MS 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 MS acquires bootstrap information from the Home Network (via the PDSN; PDSN receives this information in Access Accept). Bootstrap information includes Home address and Home agent assignment. The MS uses stateless DHCPv6 [RFC 3736] to obtain the bootstrap information from the PDSN.

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

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

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

The Home RADIUS server authenticates and authorizes the user and sends back a RADIUS Access-Accept to the HA indicating successful authentication and authorization. At this step the Home RADIUS server also distributes Integrity Key to the HA for subsequent MN-HA processing. The Integrity Key is generated using the MN-HAAA shared key and the timestamp (for randomness).

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

Assuming that proxy DAD is successful, the HA sends back a Binding Acknowledgment to the MS. In this BA message the HA includes the MN-HA mobility option, NAI mobility option and the ID mobility option. The MN-HA authenticator is calculated based on the Integrity Key that was derived in the Home RADIUS server at step e.

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)
        | (including 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,                |
        |
        |  Message ID option, MN-HA auth Options) |(10)
        |                                         |
```

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 #7
7. AAA calculates 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 auth-draft. 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 MN sent and the MN-AAA shared key. 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. Security Considerations

The security requirements for the signaling messages between the MN and HA when using the authentication option mechanism are the same as those when using IPsec to secure them.

8. Conclusion

Mobile IPv6 has been standardized only recently. Deployment of this protocol on a large scale is in the interest of the IETF and the working group as well as the 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. Hence the solution proposed in I-D draft-ietf-mip6-auth-protocol-xx.txt should be standardized by the MIP6 WG in the IETF.

9. 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 in his role as the IETF liaison to 3GPP2 has ensured that the IETF understands the 3GPP2 requirements.

10. References

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

[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.

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

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

[I-D.ietf-mip6-auth-protocol] Leung, K., "Authentication Protocol for Mobile IPv6", draft-ietf-mip6-auth-protocol-05 (work in progress), August 2005.

[I-D.ietf-mip6-mn-ident-option] Leung, K., "Mobile Node Identifier Option for Mobile IPv6", draft-ietf-mip6-mn-ident-option-02 (work in progress), February 2005.

[I-D.ietf-mip6-ikev2-ipsec]

Devarapalli, V., "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", draft-ietf-mip6-ikev2-ipsec-02 (work in progress), July 2005.

Authors' Addresses

Basavaraj Patil
Nokia
6000 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

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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