Network Working Group
Request for Comments: 5419
Category: Informational

B. Patil
Nokia
G. Dommety
Cisco

January 2009

Why the Authentication Data Suboption is Needed for Mobile IPv6 (MIPv6)

Status of This Memo

Copyright Notice

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 security association (SA) that is established between the MN and HA. The MIP6 working group has specified a mechanism to secure the Binding Update (BU) and Binding Acknowledgement (BAck) 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 is needed for Mobile IPv6 deployment in certain environments.

Table of Contents

1. 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. Such an alternate mechanism is outlined in [RFC4285]. This document is intended to capture for archival purposes the reasoning behind the need for the authentication protocol [RFC4285]. It should be noted that the alternate solution does not imply that the IPsec-based solution will be deprecated. It simply means that in certain deployment scenarios there is a need for supporting MIPv6 without an IPsec SA between the MN and HA. So the alternate solution is in addition to the IPsec-based mechanism specified in the base RFCs, i.e., [RFC3775], [RFC3776], and [RFC4877]. It has been noted that some of the challenges of deploying MIPv6 in certain types of networks arose from dependence on the Internet Key Exchange (IKE), which did not integrate well with an Authentication, Authorization, and Accounting (AAA) backend infrastructure. IKEv2 solves this problem. However, at the time of discussion on the need for the authentication

protocol, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture" [RFC4877] was still a work in progress and, as a result, an alternative solution was needed.

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.

2. 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].

3. Background

Mobile IPv6 signaling involves several messages. These include:

- The Binding Update/Binding Acknowledgment between the mobile node and the home agent.
- The route optimization signaling messages, which include the HoTI-HoT (Home Test Init/Home Test), CoTI-CoT (Care-of Test Init/ Care-of Test), and BU-BAck messages between the MN and CN. HoTI and HoT signaling messages are routed through the MN's 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 "Authentication Protocol for MIPv6" [RFC4285] provides a solution for MIPv6 deployment in environments in which an operator may not require IPsec-based security for the signaling. The reasons for an operator choosing to

deploy MIPv6 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 MIPv6 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 MIPv6 is used in such environments. It also adds additional latency to the establishment of the binding.

3. In many deployments, 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 cannot be reused for MIPv6 security as well, if IKEv1 is used.

4. Dynamic assignment of home agents is needed in certain deployments to minimize 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. In certain deployments, signaling messages between the MN and HA may be 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 MIPv6 messages does not exist.

One example of networks that have such characteristics are Code Division Multiple Access (CDMA) networks as defined in the 3GPP2 [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 MIPv6, 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 why the authentication option-based registration process for Mobile IPv6 is needed. Section 5.1 provides key arguments for the use of the authentication option. Section 5.2 provides further explanation and additional motivations for the authentication option.

5.1. Motivation for Use of the 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 operation in the [3GPP2 X.S0011-002-D] specification. 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 MIPv4 and another providing IPv6 mobility using MIPv6.

- 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.

- 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 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 AAA backend.

- 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 "MIPv6-Bootstrapping for the Integrated Scenario" [BOOT] 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, MIPv6 as specified at the time the authentication protocol was being specified, did not satisfy many of the deployment requirements. "Authentication Protocol for MIPv6" [RFC4285] along with "MN Identifier Option for MIPv6" [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 MIP4 WG. This is explained in detail in [3GPP2 X.S0011-002-D].

The earlier MIPv6 deployment model, which requires an IPsec SA that 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 RFC 4877, which enables the establishment of an IPsec SA using IKEv2 and which is also able to integrate with the backend AAA infrastructure that is responsible for the authentication of the MN in 3GPP2 and WiMAX networks.

5.2. Additional Arguments for the Use of the 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 viewed as 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. MIPv4 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 networks or WiMAX networks. CDMA2000 networks are currently deployed in many countries today. WiMAX deployments in many countries began in 2008. The packet data network architecture of CDMA2000 [3GPP2 X.S0011-002-D] includes a MIPv4 foreign agent/home agent and a RADIUS-based AAA infrastructure for Authentication, Authorization, and Accounting purposes. The AAA infrastructure provides 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 without the use of IKEv2 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 node's 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 via manual keying or established dynamically via 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 "MIPv6-Bootstrapping for the Integrated Scenario" [BOOT].

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 MN's point of attachment. While route optimization negates the benefit of having a home agent on a link close to the MN, it cannot always be guaranteed that the MN and correspondent node (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 MN's 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 infrastructure. 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 infrastructure was not specified for Mobile IPv6 at the time the authentication protocol was being specified. RFC 3776 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 -- preferably using the AAA infrastructure, 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 RFC 3776 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 backend. Since operators rely on the AAA infrastructure 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 its implementations did not meet the need of operators that were relying on 3GPP2 specifications. With the specification of IKEv2 and publication of RFC 4877, integration with AAA backends is no longer an issue.

In summary, the model of Mobile IPv6 deployment that 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- and IPv6-based mobility architectures in CDMA networks, respectively. For further details associated with the description below, please refer to Section 5, "MIP6 Operation", in the 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.

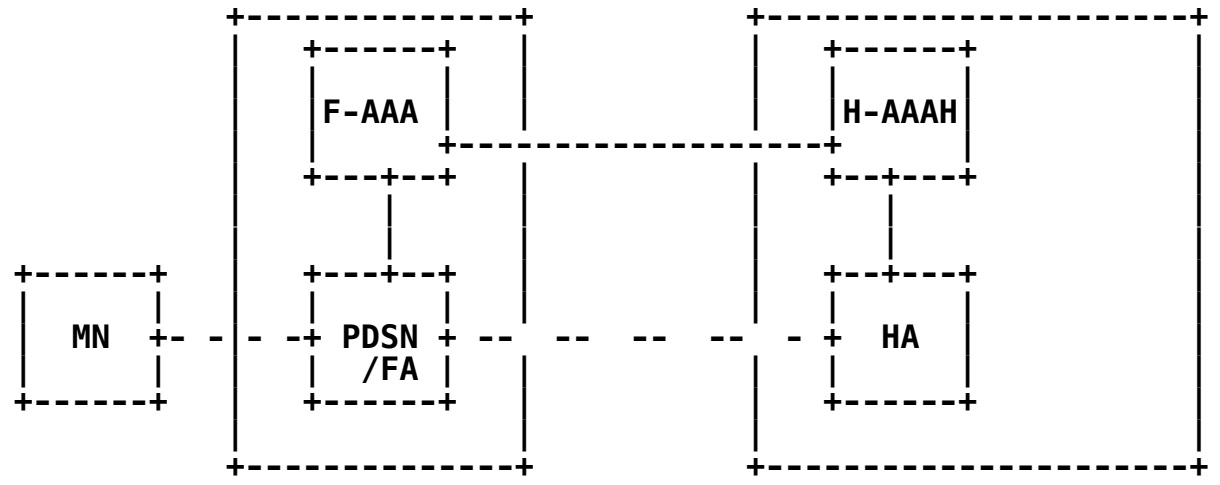

Figure 1: CDMA2000 Packet Data Network Architecture with Mobile IPv4

The CDMA mobility architecture based on MIPv4 is explained below. In this architecture, mobility is tightly integrated with the AAA infrastructure. The Mobile Node is configured with an NAI (Network Access Identifier) and an 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 the PPP on the MN/PDSN (access router link). PPP authentication is skipped. Mobile IP authentication is performed via the FA (Foreign Agent).

(2) The PDSN (Packet Data Serving Node) sends a Mobile IP challenge to the MN on the PPP link (RFC 3012).

(3) The MN sends a MIP Registration Request (RRQ), which includes the user's NAI, challenge, and MN-AAA extension that has a challenge response, and an MN-HA extension, which is generated based on the MN-HA key.

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

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

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

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

(8) The HA authenticates the RRQ (MHAE (Mobile-Home Authentication Extension)). The HA may optionally authenticate with the AAA infrastructure (just like the PDSN in #4).

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

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

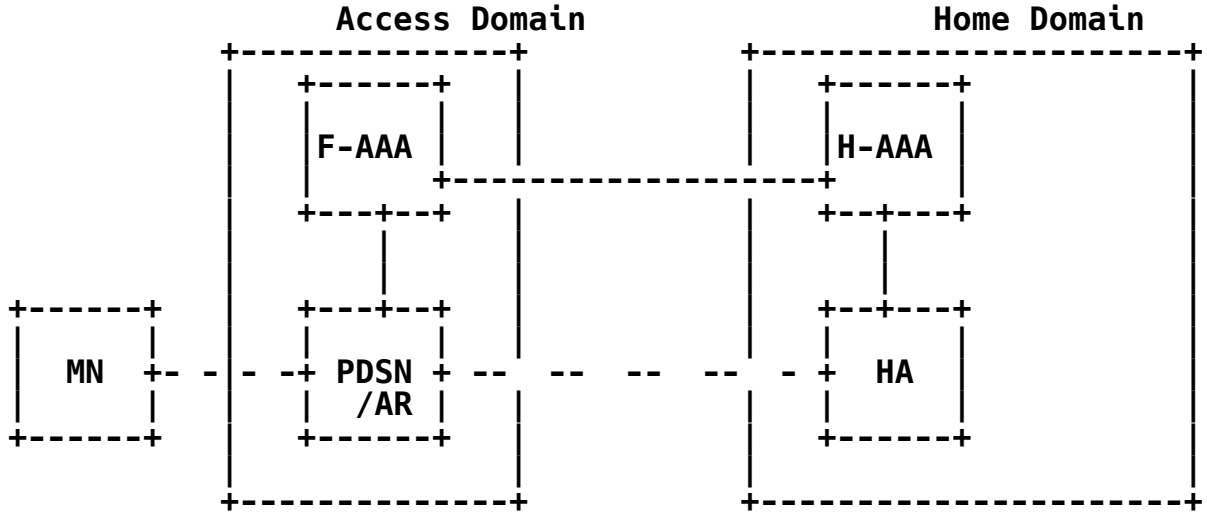

Figure 2: CDMA2000 Packet Data Network Architecture with Mobile IPv6

The Mobile Node is configured with an NAI (Network Access Identifier) and an 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 (Access Router) 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; the 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 home address (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) 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) 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 [RFC4861].

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

6.2.2. Authentication and Security Details

Access Link Setup, Access Authentication, and Bootstrapping:

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

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

(3) The H-AAA may optionally send the 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 numbers in the parentheses correspond to the explanation below):

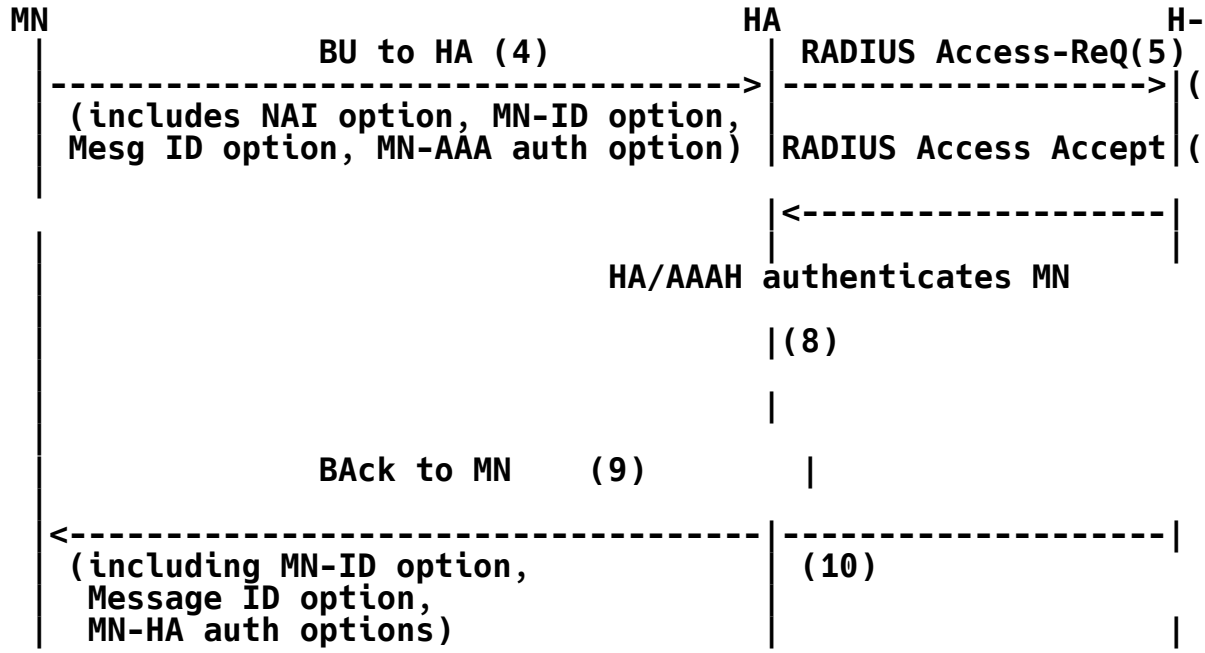

Figure 3: Flow Diagram for Initial Authentication

(4) The MN sends a Binding Update (BU) to the HA. The Binding Update is authenticated using the MN-AAA option. The authenticator in the MN-AAA option is calculated using the hash of the BU and MN-AAA shared key. It uses the HMAC_SHA1 algorithm. The Security Parameter Index (SPI) field in MN-AAA is set to 3 (as per [RFC4285]). The BU also includes the NAI and timestamp, among other details. The hash of the BU includes the 'timestamp' option and thus provides proof of liveness to prevent replay.

(5) The HA, on receiving the BU, extracts the NAI, timestamp, and authenticator from the MN-AAA option, and generates the hash of the BU. The HA sends an Access Request to the AAA and puts this information in 3GPP2-defined VSAs (Vendor Specific Attributes). The NAI is inserted in the username option in the Access Request message. The other attributes sent are: the timestamp option, the hash of the BU (till SPI field of MN-AAA auth option), and the authentication data from the MN-AAA auth option.

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

(7) AAA calculates a session key based on the MN-AAA shared secret and timestamp, and sends this to the HA in an Access Accept (in a 3GPP2-defined VSA).

(8) The HA creates a binding and a security association per Authentication Protocol for MIPv6 [RFC4285]. The key for this association is retrieved from the Access Accept and is referred to as the session key. The HA associates a fixed SPI of 5 with this SA, and is associated with the binding for the MN. (The description of this step skips the details for timestamp processing at the HA.)

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

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

The 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 the Binding Ack. If authentication is successful, the MN creates a security association with SPI=5. This key is used to authenticate further BUs to the HA using the MN-HA auth option. Once the binding lifetime expires and the 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, specifically, the same AAA infrastructure. Thus, it is natural to have similar signaling in MIPv6 as in MIPv4, 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 RFC 3775 requires a secure transport (IPsec/ESP (Encapsulating Security Payload) mode) between the MN and HA. In cases where the authentication protocol [RFC4285] is used as the means for securing the MIPv6

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 MIPv6 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 that their contents have not been modified. This implies the HA can determine the specific MN that 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 signaling 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 receive 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 Extensible Authentication Protocol (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 the 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 relies on deployment-specific mechanisms not standardized in the IETF.

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

(8) The replay protection mechanisms in [RFC4285] rely on timestamps, and thus require 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 MIPv6 signaling messages use IPsec with ESP encapsulation, they are accorded privacy on the links over which the messages traverse. When MIPv6 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 MIPv6 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. However, route optimization is not supported in the current specification of the authentication protocol in [RFC4285].

Security issues with RFC 4285 are specifically:

1. Key length. This is being addressed in [AUTH-PRO].

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 MIPv6 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. Conclusion

Mobile IPv6 was 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. RFC 4877 has alleviated some of the issues that have been of primary concern and were 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.

10. 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.

11. References

11.1. Normative References

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

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

[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.

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

11.2. Informative References

[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.

[AUTH-PRO] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", Work in Progress, July 2008.

[BOOT] Chowdhury, K. and A. Yegin, "MIP6-Bootstrapping for the Integrated Scenario", Work in Progress, April 2008.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

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

[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.

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

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