Inter-Domain Security for Mobile IPv6

Maryline Laurent-Maknavicius, Associate Professor,
INT/LOR, 9 rue Charles Fourier, 91011 Évry, France
Email: Maryline.Maknavicius@int-evry.fr
Francis Dupont, Researcher
ENST-Bretagne, 2 rue de la châtaigneraie, 35512 Cesson Sévigné, France
Email: Francis.Dupont@enst-bretagne.fr

Abstract

Mobile IPv6 is a macro-mobility "universal" solution and is only adapted to the mobile's movements within its own administrative domain. As Mobile IPv6 is expected to be the basis for the third generation cellular phone networks, a solution for inter-domain security is required. What is needed is that the visited domain should be able to authenticate the mobile to grant it access, and the mobile should identify securely the visited domain so that its communications are protected in an appropriate manner.

To solve those inter-domain security problems, new concepts known as AAA for Authentication, Authorization, Accounting were defined by the IETF. The IETF is currently defining the Diameter protocol to support those three functions in a Mobile IPv4 environment. Today's difficulty is to adapt the Diameter protocol to Mobile IPv6.

After introducing the Mobile IPv6, IPsec/IKE and Diameter protocols, this paper presents our solution and an alternative for adapting Diameter to Mobile IPv6, and gives a comparison. Both of them were published as IETF drafts in December 2001 at the Salt Lake City meeting.

Keywords: AAA, Mobile IPv6, IPv6

Mobile IPv6 [1] is a protocol designed to allow mobiles to be reached and to reach correspondents, wherever they are located, in their home network or in a visited network. As defined in draft [1], one mobile is identified thanks to a home address, and should register its new position to its home agent whenever it changes its point of attachment. Due to the inherent mobile's security problems such as mobile spoofing, and mobile's traffic redirection, Mobile IPv6 relies on security mechanisms like IPsec providing the home agent with authenticated mobile's registration information.

As it stands, Mobile IPv6 is only adapted to the mobile's movements within its own administrative domain, i.e. its domain of subscription (e.g. ISP). Indeed, no access control procedures are defined for a foreign domain to identify the mobile's administrative domain, to verify the authentication and authorizations of the mobile, and as a consequence, to be paid for the consumed network resources. As Mobile IPv6 is expected to be the basis for the third generation cellular phone networks, a solution for inter-domain security is required. What is needed is that the foreign domain should be able to authenticate the mobile to grant it access, and the mobile should identify securely the foreign domain so that its local security policy allows it to communicate with the appropriate security level.

To solve those inter-domain security problems, new concepts known as AAA for Authentication, Authorization, Accounting were defined by the IETF. Those concepts allow IP equipments – the AAA servers, the home agent and/or the mobile node - to authenticate to each other, to manage the mobile granting access, and to collect mobile connection information. The IETF is currently defining the Diameter protocol [2] to support those three functions in a Mobile IPv4 environment [3]. Today's difficulty is to adapt the Diameter protocol to Mobile IPv6.

After describing useful acronyms in section 1, sections 2, 3 and 4 introduce the Mobile IPv6 protocol, the IPsec and IKE security protocols and Diameter. Section 5 analyzes the difficulties of adapting AAA to IPv6, and gives several possible orientations. Section 6 describes our solution published as draft to the IETF to adapt Diameter to Mobile

IPv6, and section 7 presents an IETF draft alternative. Section 8 describes the remaining architecture-based security problems. Section 9 compares solutions of sections 6 and 7, and gives conclusions. Section 10 lists useful references.

1. Acronyms

AAA: Authentication, Authorization, Accounting
AAAH: Home AAA server
AAAF: Foreign AAA server
AVP: Attribute Value Pair
DHCPv6: Dynamic Host Configuration Protocol for IPv6
HA: Home Agent
ICMPv6: Internet Control Message Protocol for IPv6
IKE: Internet Key Exchange
IPsec: IP security
FA: Mobile IP Foreign Agent
MIP: Mobile IP
MIPv6: Mobile IPv6
MN: Mobile Node
NAI: Network Access Identifier

2. Mobile IPv6

Mobile IPv6 is a macro-mobility “universal” solution based on IP addresses: the **Mobile Node (MN)** has a permanent **home address** on its home link and gets temporary care-of addresses from visited links. This home address enables the MN to be uniquely identified. A router on its home link named the **Home Agent (HA)** maintains a binding cache where care-of addresses are registered.

When away from its home network, the MN should detect first that it has moved through for instance the Neighbor Discovery mechanism. That is, local routers send periodic ICMPv6 Router Advertisement messages including the link address of the router and the subnet prefix(es). The MN should then form a new care-of address using either the stateless or stateful (e.g. DHCPv6) address autoconfiguration.

The MN should register its new care-of address to its HA using the Binding Update mechanism encompassed as options of the destination extension header. The MN sends Binding Update messages to its HA until the HA returns a Binding Acknowledgement message. Then the association between the MN's home address and care-of address is named a “binding” and is registered in the HA’s cache.

After registration, the HA forwards to the MN via a tunnel packets addressed to the MN’s home address. The MN is allowed to send packets directly to its Correspondent Node (CN), with its care-of address as the source address. For its CN to identify the packet’s origin, the MN should indicate its home address in a Home Address destination option.

To avoid spoofing during registration, Mobile IPv6 requires that security parameters (i.e. security association) are negotiated between the MN and the HA. As such, in [1] all Binding Update and Acknowledgement messages exchanged between those two parties are authenticated based for instance on the Authentication Header protocol of the IPsec protocol. The next section is dedicated to the IPsec explanations and the security association negotiation protocol named IKE.

3. IPsec and IKE protocols

IPsec for "IP security" [4] is a protocol suite defined by the IETF to secure IP packet exchanges. Two new security headers are defined in IPsec, but the **Authentication Header (AH)** [5] is the only one used in Mobile IPv6 to protect Binding Update messages. The AH enables IPv6 packets to be partly authenticated, integrity protected, and optionally protected against packet replays. Several mechanisms and parameters are available for that header, and should be negotiated prior to securing packet exchanges. The resulting parameters of that negotiation are named **IPsec security associations** and usually encompass a secret key, an algorithm, and a lifetime for that security association. Those parameters are referred to as **keying material** in sections 6 and 7.

Security associations may be done either manually on each equipment, or automatically using the **IKE (Internet Key Exchange)** protocol [6]. IKE requires two phases of negotiation. Phase 1 results in the sharing of a high-level security association which enables IKE exchanges of the second phase to remain confidential. Phase 2 named **"quick mode"** is based on a three-way message exchange protocol, and enables remote equipments to negotiate security associations for IPsec implementation.

It should be noted that IPsec support is mandatory in IPv6, and thus enables any pair of IPv6 equipments to protect their communications.

4. Diameter

The Diameter protocol which implements the AAA concepts [7] for MIP, and is used when the mobile is away from home includes a base protocol [2] which defines the PDU format in the form of **Attribute Value Pairs (AVP)**. Some AVPs are base protocol oriented. Others should be defined for use in the Mobile IPv6 or Mobile IPv4 [3] context.

Diameter is based on a specific architecture including the Mobile IP entities (MN, HA) and three AAA entities which are:

- Home AAA **(AAAH)** server is located in the MN’s home/remote network. It authenticates the MN and gives authorization to the MN to register to a specific HA. AAAH may also distribute keys to Diameter entities.
- Foreign AAA **(AAAF)** server is located in the MN’s

visited/local network. If unable to process the MN authentication locally, it forwards the authentication requests to the AAAH.

- Attendant is a node providing a service interface between the MN and the AAAL. In Mobile IPv4, the attendant is the Foreign Agent.

In Diameter, MN is uniquely identified by a NAI (Network Access Identifier) in the form user@localdomain. NAI is used by the AAAF to identify the AAAH to which the MN belongs (based on the localdomain information). The MN authentication is then performed by AAAH which should authorize or forbid a MN to connect to the foreign domain.

Diameter works as illustrated in figure 1. MN sends a Registration Request MIP message to FA which constructs a Diameter AMR (AA-Mobile-Node-Request) message including this Registration Request message (in the MIP-Reg-Request AVP), the MN's home address, the MN's NAI and the HA's identity. The AMR message is then forwarded to AAAF which decides whether the AMR may be locally processed or should be forwarded to AAAH. Actually, FA uses the AAA infrastructure to authenticate and authorize the MN to connect locally.

Once MN is authenticated, AAAH sends a Diameter HAR (Home-Agent-MIP-Request) message to HA which contains the MN's Registration Request message. HA checks the validity of the HAR message, proceeds the Registration Request message, and constructs a Registration Reply. The latter message is forwarded to MN hop-by-hop, first encapsulated in the HAA Diameter message, and then in the AMA Diameter message, and finally as a Registration Reply MIP message.

MN may have no HA and/or no home address. AAAH is then allowed to allocate an HA and a home address depending on its own security policy, and such information is returned to MN through the AMA message. The home address may also be allocated by HA.

AAA entities are allowed to negotiate security associations to protect future AAA exchanges using specific security application oriented AVPs. Security services offered are entities authentication, and AAA message confidentiality and integrity.

5. Difficulties to adapt AAA to Mobile IPv6

When adapting AAA to Mobile IPv6, the idea is to optimize the network bandwidth and delays when the MN requests access to the foreign link. Indeed, many protocols are involved at that time including Mobile IPv6, IPsec, IKE (cf. section 3), AAA, and optionally DHCPv6 and/or ICMPv6 for address autoconfiguration. As it stands now, the MN first should be authenticated by the AAA servers to get access to the foreign link (AAA protocol). Then it may proceed the address autoconfiguration (ICMPv6, DHCPv6) to get a care-of address, and negotiate a security association (IKE) with the selected HA prior to sending a Binding Update (Mobile IPv6, IPsec). At least ten messages should be exchanged between MN/AAAF (2 messages), and MN/AH (6 IKE messages and 2 Mobile IPv6 messages). For optimization purpose, one solution is to piggy-back payload of some of those protocols (IKE, Mobile IPv6) into AAA messages and AAA payload exchanged between the MN and the attendant (AAA access server, cf. section 4) into DHCPv6 or ICMPv6 messages.

One difficulty in Mobile IPv6 is the absence of Foreign Agents which are defined in Mobile IPv4. As such, the Mobile IPv6 architecture does not map easily to the AAA architecture. One possibility to force the MN to connect to a server prior to transmissions is to combine the attendant function with the address autoconfiguration procedure. For

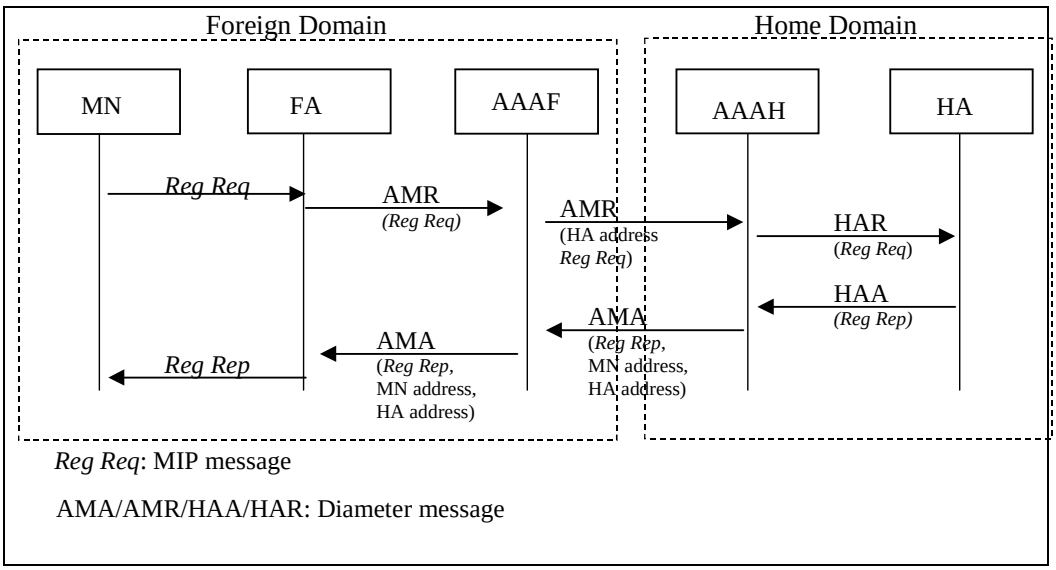


Figure 1. *Diameter exchanges if MN connection to a foreign domain is successful.*

the stateful autoconfiguration, the attendant is hosted in the DHCPv6 server, and for the stateless autoconfiguration based on the ICMPv6 protocol, the attendant is hosted in the ICMPv6 module within a local router. The problems of such approaches are described hereafter.

The ICMPv6 approach should define new ICMPv6 messages to carry AAA and Mobile IPv6 payload between the MN and the attendant. The problem is that ICMPv6 is a pretty stable protocol described in RFC 2463 (December 1998). As such, it is highly likely that the IPng Working Group in charge of the ICMPv6 standardization will be reticent to introduce modifications.

The DHCPv6 approach requires at least new DHCPv6 options. One solution based on this approach [8] was presented to the IETF in March 2001. The idea of [8] is to piggy-back Diameter and IKE-like payloads into the DHCPv6 exchanges between the MN and the DHCPv6 server, and IKE-like payload into the Diameter messages exchanged between the DHCPv6 server, AAA servers and the HA.

The DHCPv6 approach offers one advantage over the ICMPv6 one. The MN is expected to wait until the DHCPv6 server allocates one care-of address and gets authorization from the AAA infrastructure. In the ICMPv6 approach, the MN receives periodic Router Advertisements messages and is then able to construct its own IPv6 address and to transmit data packets directly over the network. If correctly configured, the local router should reject those packets, but anyway, stations or servers located to the same link, if any, are still reachable by the MN.

For the AAA solution to apply to any IPv6 address autoconfiguration procedures, both current IETF proposals described in the next two sections remain independent of the protocol used between the attendant and the MN to support AAA exchanges. Moreover, the attendant does not necessarily map to the DHCPv6 server or the local router.

6. Our IETF proposal

The idea of this adaptation [9] described in figure 2 is to piggy-back Diameter and IKE-like payloads into IPv6 exchanges between the MN and the attendant, and IKE-like payload into the Diameter messages exchanged between the attendant, AAA servers and the HA. Because only two round trips are available between HA and MN, the IKE protocol is not usable as it is described in section 3. The IKE-like protocol considered in [9] for security association negotiation can be a light IKE protocol, that is for instance the IKE quick mode phase 2 truncated to its first two messages.

The protocol used between the attendant and MN can be any protocols satisfying the following three properties: it should be based on two phases (Attendant Solicit/Advertisement and then Attendant Request/Reply); the advertisement message contains a local challenge; and the protocol can carry AAA payloads.

The adaptation solution in [9] is flexible in that the MN's home address and the HA can be allocated dynamically by AAAH. Moreover, this approach is adapted to any address autoconfiguration procedures as MN is allowed to compute locally its care-of address (Co@) or should wait until allocation is done by the attendant. As such, the care-of address parameter is optional in the Attendant Reply message.

The aim of [9] is to describe the basic principle of the solution without any implementation details such as new AVP required, possible algorithms, etc.. As such, the content of the information exchanged is roughly described in table 1.

AAA messages considered in [9] and extracted from Diameter (cf. section 4) include:

- AMR (AA-MN-Request): AAA message from the attendant to AAAH via AAAF. This is the first AAA message sent to request access for MN.
- AMA (AA-MN-Answer): AAA message from AAAH to the attendant. This is the final AAA message.
- AHR (AA-HA-Request): the second AAA message from AAAH to HA.
- AHA (AA-HA-Answer): the third AAA message from HA to AAAH.

This approach assumes that above AAA messages are secure benefiting from the security supported by the AAA protocol (cf. section 4). That is, AAA offers the AAAH, AAAF and attendant the means to authenticate to each other. To do that, the MN is assumed to know the AAAH's public key and the AAAH the MN's public key. In [9], in absence of the HA's address in the AMR message, one HA may be allocated by AAAH to an MN.

Approach [9] provides the AAA infrastructure with the following services:

- Replay protection ensured by the attendant and the AAAH

  Either timestamps or random challenges are used for replay protection. The first one requires a synchronized clock and consists for the AAA receiver to check the timestamp of the received message against its local clock. For the second one, AAAH and MN have to maintain two Replay Protection Indicators RPI1 and RPI2 in a cache. RPI2 is randomly generated by MN prior to transmitting an Attendant Request so that the freshness of the corresponding AAAH reply is checked. AAAH also verifies the freshness of the requests from MN thanks to RPI1 it generated. The AAA updates its RPI1 with RPI1'.

  The attendant should locally protect against replays of Request messages by checking the Local Challenge (LC)

in the Request against the LC it previously sent.

It should be noted that the replay protection is only possible in conjunction with the authentication service provided by AAAH.

Fields	Content
Aaa_key	MN issued keying material (encryption algorithm, secret and lifetime) for the security exchanges between MN and AAAH
BA	Mobile IPv6 acknowledge for the binding update message
BU	Mobile IPv6 Binding Update
attendant_key	MN issued keying material for the security exchanges between the attendant and MN
CR	MN's AAA credential which is used by the AAAH to authenticate the MN. The CR is bound to the AMR content. CR is suggested to be computed with asymetric cryptography like RSA
SecuParam_I	Security Association establishment elements from initiator/MN
SecuParam_R	Security Association establishment elements from responder/HA
LC	Local challenge issued by the attendant
NAI	MN's identity
pub_key	AAAH 's public key
RPI	Time-stamp or nonce used between the MN and the AAAH to ensure replay protection
H@	MN's home address is present in AHR/AHA and either in AMR (if known by MN) or AMA (if allocated by AAAH)
HA@	HA's address is present in AHR/AHA and either in AMR (if known by MN) or AMA (if allocated by AAAH)
RC	AAA result code (in AAA answers)

Table 1. *Fields used in solution [9]*.

- Authentication

The MN (and/or the user) identified by its NAI (Network Access Identifier) and/or its home address (H@) is authenticated by AAAH thanks to the digital signature included in the credential (CR) of the Request message. The credential securely binds the AAA data included in the MN's Request and provides a secure replay protection.

MN has the proof of identity of AAAH since AAAH is the only one able to decipher the {aaa_key}pub encrypted with its public key (pub_key) and to encrypt data (SecuParam_R) with the deciphered result aaa_key.

MN proceeds to a delayed authentication of the attendant based on the attendant_key material.

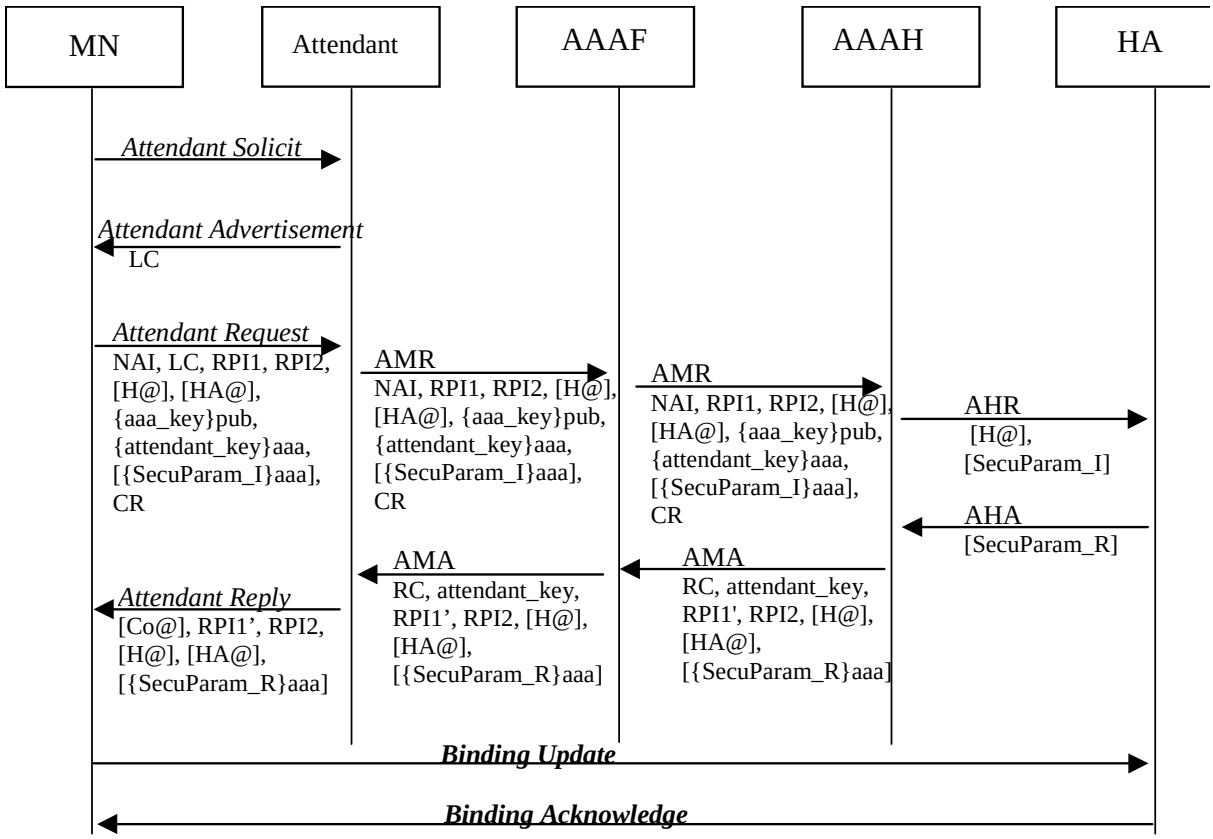
- Security association negotiation

As no IPsec security associations may be available between the MN and the HA, and Binding Update/Acknowledgement may require IPsec AH protection (cf. section 2), it is required that a IPsec security association is agreed between parties. This is usually done by the Internet Key Exchange (IKE) protocol. What we suggest here is to reuse part of the IKE code. More precisely, we limit the negotiation to the first two exchanges (SecuParam_I and SecuParam _R) of the IKE three-way protocol (quick mode of phase 2). The last IKE exchange is used for the MN's liveliness and is redundant with the replay protection offered by our approach.

- Confidentiality of security parameters

The MN sends one locally-generated key (aaa_key) to the AAAH enciphered using the asymetric AAAH's public key (pub_key). The keying material aaa_key (either symetric or asymetric cryptography-based) is used to exchange confidential data between AAAH and MN, such as the SecuParam_I, SecuParam_R and attendant_key.

possibility is that no means are given for the AAAH to know the MN's care-of address and as such AAAH seems



Notations:

[XX]=Optional element XX

{XX}xxx=Protected element XX using the xxx_key keying material (algorithm, secret key and lifetime)

Message between MN and the attendant: IPv6 messages (no specific protocol defined)

Message AMR, AMA, AHR, AHA: AAA messages

Binding Update/Acknowledge: Mobile IPv6 messages

Figure 2. *Exchanges considered in draft [9]*.

7. An alternative IETF proposal

Like draft [9], draft [10] is independent of the protocol used between the attendant and the MN to support AAA exchanges. The main idea of [10], as described in figure 3, is to give the possibility to piggy-back Mobile IPv6 payload and some keying material into Diameter messages. That is, if the MN is provided with a HA and shares a security association with it, the MN may create a Binding Update (BU) encompassing its care-of address and encapsulate it to its HA via the attendant. Otherwise, the AAAH assigns an HA (HA@), creates a BU, and sends it to the HA along with some keying material (key-info) that must be used by the HA to authenticate MN's future Binding Updates. One of the problems of the latter not able to generate a correct Binding Update.

This solution gives implementation details defining four new Diameter messages and eight new AVPs, however it remains unclear regarding the content of the key-info field encompassing keying material information. What is expected at the end of the exchanges is that keying material is shared between MN and HA, and between MN and the attendant.

Fields	Content
BA	Mobile IPv6 aknowledge for the binding update message
BU	Mobile IPv6 Binding Update
CR	MN's credential used by AAAH for MN's authentication
H@	MN's home address is present in HOR/HOA and either in ARR (if known by MN) or ARA (if allocated by AAAH)
HA@	HA's address is present in HOR/HOA and either in ARR (if known by MN) or ARA (if allocated by AAAH)
HC	Host challenge issued by MN
key-info	Any keying material oriented information in order to establish keying material between MN/attendant, and MN/HA
LC	Local challenge issued by the attendant
NAI	MN's identity

Table 2. *Fields used in solution [10]*.

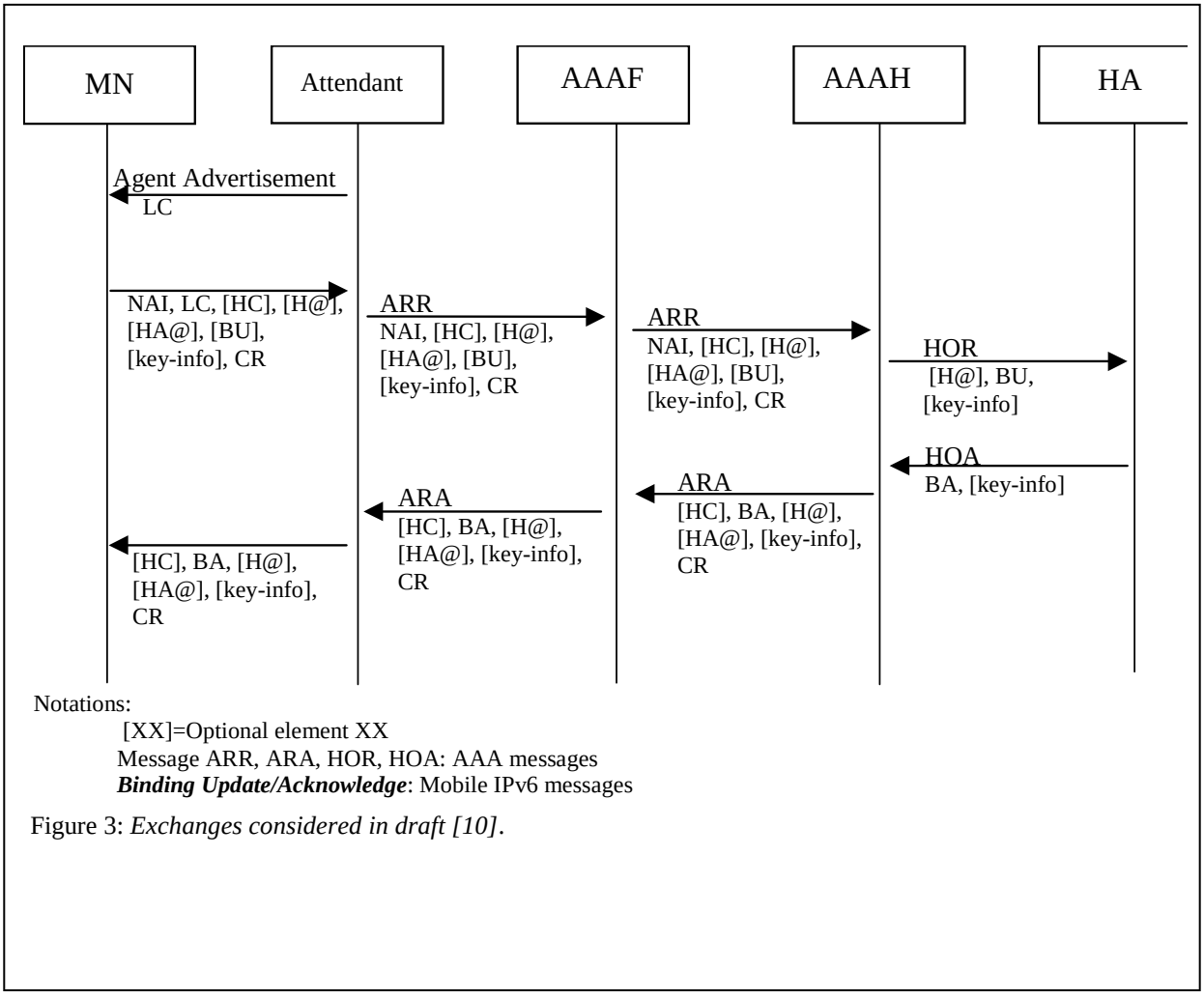
New Diameter messages include:

- ARR (AA-Registration-Request), a message equivalent to the AMR message of draft [9],
- ARA (AA-Registration-Answer Command), an AMA-equivalent message,
- HOR (Home-Agent-MIPv6-Request Command), an AHR-equivalent message,
- HOA (Home-Agent-MIPv6-Answer Command), an AHA-equivalent message.

Drafts [10] and [9] are quite similar. Like in [9], the Local Challenge (LC) field is used by the attendant to verify the freshness of the MN's request and to detect any replays. The optional Host Challenge (HC) generated by MN is equivalent to the RPI2 challenge of draft [9], but no mechanism equivalent to RPI1 is available for AAAH to detect replays. For replay detection, AAAH relies on the replay detection performed by the attendant. The Home address (H@) and the HA address (HA@) indicated by MN are optional since they may be dynamically allocated by AAAH.

The Binding Update message (BU) is either generated by MN if MN knows its HA, otherwise AAAH generates one

-



Notations:

[XX]=Optional element XX

Message ARR, ARA, HOR, HOA: AAA messages

Binding Update/Acknowledge: Mobile IPv6 messages

Figure 3: *Exchanges considered in draft [10]*.

and sends it to HA through a HOR message in place of MN. HA replies with a Binding Acknowledgement message (BA) which is forwarded to MN hop-by-hop.

8. Remaining security problems

In spite of the AAA introduction, architecture-based security problems still remain.

To preclude any MN to bypass the AAA authentication and authorization procedures and access to network resources, it is necessary that dynamic access lists within the access router are configured to filter the traffic. Those access lists should be defined in conjunction with the attendant so that only authorized MNs are able to transmit traffic through the router. This requires that the attendant is hosted in the router or is connected to the router through the monitoring port and updates the access lists each time a new MN is successfully authorized to access the network or is leaving the network. This is of high importance that the access lists are updated when the MN is leaving the network to avoid another MN be configured with the same address and benefits of the same rights.

The visited domain should give the MN in visit a restrictive access to its applications to avoid sensitive data disclosure.

9. Comparisons and conclusions

This paper describes two IETF proposals to adapt AAA to the Mobile IPv6 environment: the draft of Le et al. [10] and our draft [9]. Both of these drafts enable keying material information for security association establishment to be piggy-backed into AAA exchanges. However, [10] is the only one performing the piggy-backing of Mobile IPv6 data into the AAA protocol.

Several elements of comparisons between solutions [10] and [9] are given hereafter. [10] is more restrictive than [9] since only the stateless address autoconfiguration procedure is supported. Contrary to [9], [10] does not apply if MN boots for the very first time in a visited network since the home AAA server (AAAH) and MN are assumed to initially share a long-term key. Like [9], [10] is flexible enabling the MN's home address and HA to be dynamically allocated by the AAA infrastructure, but with the additional possibility for HA to be located in the visited network. Moreover, [10] enables MN to be authenticated strongly by AAAH based on authentication protocols requiring more than two-way exchanges, but the implementation is not detailed. The home domain in [10] relies on the replay detection performed by the attendant, and appears as not secure since the attendant should not be necessarily trusted. Finally, [10] assumes that AAAH generates a Binding Update if MN is not provided with a home address, but no means for AAAH to be informed of the MN’s care-of address are presented.

Adapting Diameter to Mobile IPv6 appears as a fundamental challenge for the third generation cellular network deployment (e.g. UMTS, CDMA) as future cellular networks are expected to be IPv6-based providing mobiles with data packet transport services. Moreover, the AAA architecture proposed by the IETF is particularly suitable for a large mobile network, enabling ISP with the help of other ISPs to authenticate users and grant them access. Today, access may be granted according to the users subscription type, the quality of service requested over the connection, etc.. As AAA was designed for filtering access at the mobile connection request only or during mobile's moves, one evolution of the AAA architecture would be to perform filtering on the telecommunication services required by the user, or the called phone numbers, but this assumes modifications so that the AAA architecture is solicited for each new service/phone number contacted by the mobile.

10. References

[1] D.B. Johnson, C. Perkins, "Mobility Support in IPv6", Internet draf draft-ietf-mobileip-ipv6-15.txt, July 2001.

[2] P.R. Calhoun, H. Akhtar, J. Arkko, E. Guttman, A.C. Rubens, G. Zorn, "Diameter Base protocol", Internet draft draft-ietf-aaa-diameter-07.txt, July 2001.

[3] P.R. Calhoun, Charles E. Perkins, "Diameter Mobile IPv4 Application", Internet draft draft-ietf-aaa-diameter-mobileip-07.txt, July 2001.

[4] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Nov. 1998.

[5] S. Kent, R. Atkinson, "IP Authentication Header", RFC 2402, Nov. 1998.

[6] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, Nov. 1998.

[7] C.E. Perkins, "Mobile IP Joins Forces with AAA", *IEEE Personal Communications*, Vol. 7, No4, Aug. 2000, pp 59-61.

[8] F. Dupont, M. Laurent-Maknavicius, "AAA for mobile IPv6 ", Internet draft draft-dupont-mipv6-aaa-00.txt, Feb. 2001.

[9] F. Dupont, M. Laurent-Maknavicius, J. Bournelle, "AAA for mobile IPv6", Internet draft draft-dupont-mipv6-aaa-01.txt, Nov. 2001.

[10] S.M. Faccin, F. Le, B. Patil, C.E. Perkins, "Diameter Mobile IPv6 Application", Internet draft draft-le-aaa-diameter-mobileipv6-01.txt, Nov. 2001.