Using PANA for Mobile IPv6 Bootstrapping

Julien Bournelle[1], Jean-Michel Combes[2], Maryline Laurent-Maknavicius[1], and Sondes Larafa[1]

[1] GET/INT, 9 rue Charles Fourier, 91011 Evry, France
julien.bournelle@gmail.com
Maryline.Maknavicius@int-evry.fr
sondes.larafa@gmail.com
[2] France Telecom R&D, 38/40 rue du General Leclerc,
92784 Issy-Les-Moulineaux, France
jeanmichel.combes@orange-ftgroup.com

Abstract. One of the current challenge of the Mobile IPv6 Working Group at the IETF is to dynamically assign to a Mobile Node its Home Agent, Home Address and to setup necessary security associations. If the Mobile Node is authenticated for network access, the current IETF approach is to use DHCPv6 to deliver the Home Agent and then to use IKEv2.

In this article, we assume that the PANA protocol is used for network access authentication. We propose to add some functionalities to this protocol to support Mobile IPv6 Bootstrapping. The Home Agent is directly delivered to the Mobile Node and DHCPv6 is no more necessary. Moreover, it allows a better management of Home Address allocation by the AAA infrastructure.

This proposal has been submitted to the IETF and implemented on a testbed at GET/INT research laboratory.

1 Introduction

In the Mobile IPv6 protocol, a Mobile Node needs a Home Agent, a Home Address and IPsec Security Associations with its Home Agent to secure signaling messages. To ease the deployment of this mobility protocol, Internet Service Providers need scalable mechanisms to dynamically assign these pieces of information to their customers. This is known as the *Mobile IPv6 Bootstrapping Problem*. In this paper, we propose a solution based on the PANA protocol to deliver the Home Agent Information to the Mobile Node during the network access authentication phase.

In section 2, the Mobile IPv6 protocol is presented. Section 3 describes the Mobile IPv6 Bootstrapping problem and the IETF bootstrapping solution based on the DHCPv6 protocol. Our solution which relies on the PANA protocol is detailed in section 4. Finally, this proposal has been implemented and a description of our testbed is given in section 5.

I.F. Akyildiz et al. (Eds.): NETWORKING 2007, LNCS 4479, pp. 345–355, 2007.

2 Mobile IPv6 Overview

As it stands in [1], an IPv6 Mobile Node (MN) is uniquely identified by its Home Address (HoA), and is maintained reachable, whatever its position in the IPv6 network, thanks to a registration mechanism to its Home Agent (HA). Each time the MN attaches to a new network after some moves or reboots, the mobile is assigned a new local temporary IPv6 address either from a DHCPv6 server or through address autoconfiguration. The MN then has to inform its Home Agent of its temporary address also known as its Care-of Address (CoA). This operation of binding its HoA to its CoA is operated by the MN sending a Binding Update (BU) and the HA acknowledging the BU message with a Binding Acknowledgement (BA) (cf. Fig. 1). After the registration is completed, the HA intercepts all the data traffic directed to the HoA, and tunnels them to the current position of the MN (i.e. CoA). Thus any Correspondent Node (CN) only needs to know the HoA to transmit data to MN via HA. For Routing Optimization (RO) purpose, the Mobile IPv6 protocol enables CN and MN to directly communicate rather than going through HA.

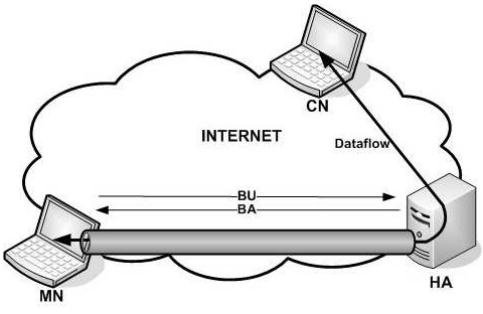

Fig. 1. Mobile IPv6 architecture

Binding operations are highly sensitive to malicious traffic redirections, and do require strong protection. For binding updates operated by MN to HA, protection is guaranteed by the IPsec sub protocol ESP (Encapsulating Security Payload) in transport mode [2]. HA is thus enabled to authenticate the BU's originator, and to prove the integrity of the BU content, especially the CoA which is located within the Alternate Care-of Address mobility option. However, this ESP mechanism assumes that a Security Association (SA) is pre-established between HA and MN (MIPv6 SA).

For the binding updates operated by MN to CN, the mechanism is less secure as no strong assumption on a preshared Security Association might be imposed. The selected mechanism known as Return Routability [1] proposes that MN sends two messages to CN, one directly to CN and another one through HA, and that the two replies from CN follow the reverse path. The idea is that intercepting two messages instead of one to perform one possible traffic redirection is much

more difficult. Moreover, because of ESP protection between HA and MN, HA brings a guarantee to CN about the authenticity of the request.

3 The Mobile IPv6 Bootstrapping Problem

3.1 Problem Description

As explained in section 2, the Mobile IPv6 service needs for activation that the Mobile Node be pre-configured with a HA, a HoA and MIPv6 IPsec SA with the Home Agent to protect Mobile IPv6 signaling. Note that another mechanism exists based on an authentication option to secure this signaling [3] but it is not considered in this article. These parameters may be statically configured on each Mobile Node. However, considering an operator willing to deploy the Mobile IPv6 protocol inside its IP networks, static configuration of millions of electronic devices is a burden and clearly not scalable. Moreover, as explained in [4], other reasons state for a dynamic bootstrapping mechanism:

- Dynamic Home Agent assignment: to offer the Mobile IPv6 service, an operator will deploy multiple Home Agents. For load balancing between HAs, the less loaded HA should be allocated to MNs. Moreover, if a HA becomes unavailable for maintenance, network renumbering or failure, with a dynamic assignment, the operator is still able to provide the service.
- Dynamic Home Address assignment: the operator may want do dynamically assign Home Address to its clients. Indeed, this is preferred for a better management of address allocation and to ease administrators' tasks.

The current trend at the *Internet Engineering Task Force* (IETF) is to first attribute the Home Agent to the Mobile Node and then to proceed to IKEv2 [5] exchanges between the MN and the HA. IKEv2 enables the MN to query a Home Address and, in the same time, to dynamically setup the MIPv6 SAs with its HA, as required by Mobile IPv6. Moreover, IKEv2 supports the EAP protocol [6] for the HA to authenticate the MN. Use of EAP permits the MN to use the same credentials that have been used for network access authentication (if any).

Two generic scenarios are possible [4]: in the first one, the Mobile Node has a free network access (e.g. hotspots in a coffee shop) while in the second one, the MN is authenticated before getting network access. For the first scenario, the IETF proposed delivering the HA information through DNS infrastructure [7]. In the second scenario, the Home Agent information is delivered as part of the network access authentication procedure [8]. In both scenarios, the MN then uses IKEv2 with the delivered Home Agent.

In this article, we assume that the Mobile Node is in the second scenario. As described in [8], the IETF approach is to use DHCPv6 [9]. In our proposed mechanism, we can bypass DHCPv6 exchanges by delivering the HA information during the network access.

3.2 DHCPv6 Approach

One way to attribute the Home Agent for MN bootstrapping, relies on the re-use of the network access control architecture. At the same time the MN asks for the IP access to the operator's network, it recovers the Home Agent. The IETF is working on a solution described in [8] using the DHCPv6 protocol [9]. Figure 2 shows the entities involved in this solution.

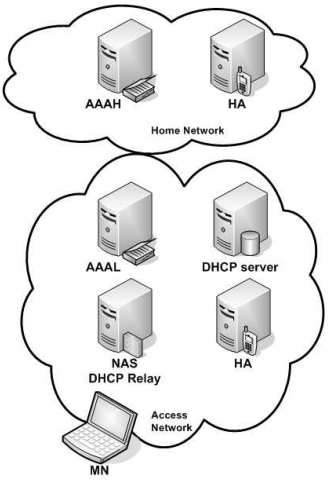

Fig. 2. MIP6 Bootstrapping with DHCPv6: architecture

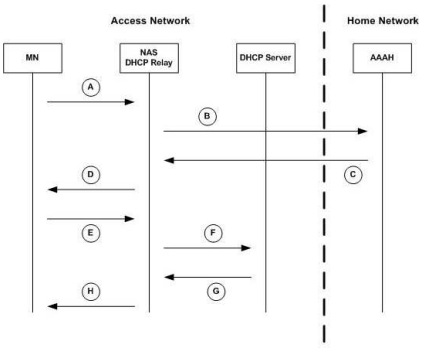

Fig. 3. MIP6 Bootstrapping with DHCPv6: exchanges

Figure 3 presents the different steps of this solution. At first, the MN authenticates itself to the Network Access Server (NAS) with a protocol like PANA or 802.11i/802.1X (Step A). The NAS asks the AAA server in the Home Network (AAAH) about the MN's rights (Step B). The AAAH checks in the same time whether the MN subscribed to the IPv6 mobility service. If this is the case, the

AAAH replies to the NAS that the MN is allowed to access the network and which HA to be used (Step C). Then the NAS informs the MN it can access the network and stores the information about the HA assigned by the AAAH (Step D).

To obtain the HA, the MN then sends a DHCP request (Step E). The NAS, which must also act as a DHCPv6 Relay, intercepts the request and forwards it to the DHCP server, adding the information about the HA assigned by the AAAH (Step F). If the MN required a HA in the local network, the DHCP server assigns a HA. If the MN required a HA in the Home Network, it is the one assigned by the AAAH. The DHCP sends the information about the HA to the NAS (Step G) which forwards the reply to the MN (Step H).

4 PANA Approach

4.1 PANA Overview

PANA (Protocol for Carrying Authentication for Network Access) [10] is currently under standardization by the IETF and appears as a good candidate for handling MNs authentication at the network access as it is layer 2 agnostic, and it supports any EAP methods. Based on the client server model, the classical PANA architecture (cf. Fig. 4) utilizes a PANA client (PaC) located in the MN and a PANA Authentication Agent (PAA) located in the network access for instance in the access router (or NAS). For controlling MNs access to the network, an EP (Enforcement Point) should apply security and filtering policies at levels 2 and/or 3, so only authenticated and authorized MNs are permitted to send data traffic to the access network; EP is located at the access network and possibly on the same equipment than the PAA.

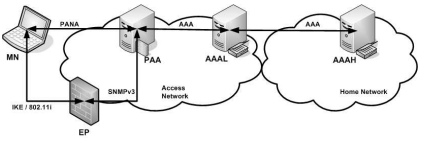

Fig. 4. PANA framework

Several phases are necessary for the MN to connect to the access network. First, the PaC needs to discover the local PAA, and negotiate services. This first phase includes classically three messages. Second for PAA to proceed to authentication of MN, some PANA messages are exchanged encapsulating EAP payloads. This authentication/authorization phase might rely on a AAA architecture handling authentication thanks to AAA servers and a AAA client located on the same equipment than PAA. Third, the MN is granted access to some Internet resources through the EP, but PANA messages are still exchanged for session

keep alive reasons. From time to time, reauthentication of MN is required by the PAA or the AAA servers. All these PANA messages and AAA messages are in the form of AVPs (Attribute Value Pair).

4.2 Using PANA for MIP6 Bootstrapping

Without any modifications, in the case of a Mobile Node using PANA for network access authentication, exchanges would be first the PANA exchanges, then DHCPv6 to get the HA and then IKEv2. Our idea is to modify PANA in order to negotiate and to deliver Mobile IPv6 information to the Mobile Node. For this purpose, we introduced new AVPs in PANA messages.

We defined a new *Attribute Value Pair* (AVP) called `Mobility-Capability` AVP. This AVP is used by the PANA Authentication Agent (PAA) to indicate to the MN/PaC that it supports Mobile IPv6 Bootstrapping. This AVP may be used to indicate other IP mobility capabilities such as Mobile IPv4 [11] or HIP [12]. This AVP is sent in the first `PANAStart-Request` message (PSR) as shown on Fig. 5. If the Mobile Node supports our proposal and wants to bootstrap IPv6 Mobility service, it includes the `Mobility Capability AVP` indicating its willingness in the `PANA-Start-Answer` message (PSA). This AVP may also be used to indicate whether the MN wants a local HA or a HA in its home domain. Compared to the DHCPv6 approach, this permits to the AAAH server to decide whether the MN is allowed to use a local HA.

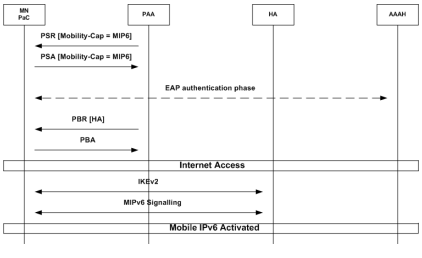

Fig. 5. MIP6 Bootstrapping with PANA: exchanges

After this negotiation phase, we enter the authentication phase. The PAA relies on a AAA protocol to authenticate the MN. As described in [13] or in [14], the AAA signaling may be used by the PAA to indicate that it supports Mobile IPv6 Bootstrapping. Moreover, the visited domain may also indicate that it can locally allocate a HA. At the end of the authentication phase, the PAA obtains the HA information in the AAA message containing the result of the authentication. Note that if the authentication failed, it is not necessary to provide the HA information to the NAS (e.g. PAA).

To deliver the HA to the MN, the PAA creates an AVP `Home-Address` (HoA) and puts it in the `PANA-BindRequest` message (PBR). Thus, at the end of the authentication, the MN has its Home-Agent and can use IKEv2 to get its Home-Address and to setup necessary IPsec SAs.

4.3 Pros and Cons

The main advantage regarding our solution is that it keeps the "end-to-end" Internet philosophy. Indeed, in our solution, the MN knows that it will receive a HA and it might be guaranteed that this HA assignment is done by its AAAH (e.g. thanks to encryption mechanisms). In the DHCP based solution, the information about the HA is stored in the DHCP server and the MN cannot be totally sure that the information about the assigned HA comes from the Home Network.

Another advantage is that the AAAH server can decide if the Mobile Node can use a local HA. Indeed, in our approach, this is managed at the beginning of the authentication phase. In the DHCPv6 approach, only the MN can decide if a local HA is required.

Regarding the cost of our solution, this one does not require setting-up a DHCP infrastructure (i.e. client in the MN, relay in the NAS and server in the access network), so this reduces the cost of the Mobile IPv6 deployment. Moreover our solution may support privacy because it may be possible for the AAAH to cipher the information about the assigned HA up to the MN.

Finally, our solution is naturally secured regarding the authentication and the integrity of the data because the security relies on PANA. This may not be the case for DHCPv6.

Now, even if our solution reduces the allocation of the HA in one roundtrip time and provides hereabove advantages, the IETF is against the fact that network access control protocols support configuration.

5 Implementation Report

5.1 Required Adaptation for the Implementation

Our proposal has been submitted to the IETF in [15] and can be integrated in the overall architecture of the proposed IETF solution. However, due to some external constraints, the implementation is different from the original proposal. The differences are explained in this section.

At the time of implementation, no IKEv2 with EAP and Mobile IPv6 support was available. For this reason, we used IKEv1 [16]. However, IKEv1 does not permit to remotely configure the IPv6 address of its MN clients. For this reason, in our platform, the AAA server handles the Home Address Allocation and sends it to the PAA. Then the Home Address is carried to the MN using PANA messages.

Normally, IKEv2 allows use of EAP to authenticate the MN. In IKEv1, only certificates or pre-shared keys permit to authenticate the IKEv1 exchanges. For this reason, we decided to bootstrap and distribute keying material for IKEv1 authentication between MN and HA. Our solution is to derive the PSK from the Master Session Key (MSK). This MSK is derived as part of the EAP authentication method and is available at both EAP client (MN) and EAP server (AAAH). Due to the colocation of HA and AAAH, the resulting PSK for IKEv1 is easily configured by modifying IKEv1 configuration file.

5.2 Platform

The hosts A, B and C use FreeBSD 5.4[1] as operating system. As shown on Fig. 6, the MN is installed on host A, the host B acts as an Access Router and implements PAA and AAA client functionalities, and finally the AAA and EAP servers, colocated with the HA, are installed on host C. Details are given in next subsections.

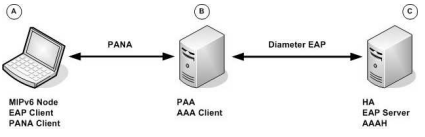

Fig. 6. PANA - Mobile IPv6 testbed

5.3 Mobile Node

The host A was installed with SHISA[2] to support Mobile IPv6, an EAP client, a PANA client and IPsec components (IKE, AH and ESP). The EAP client was extracted from *xsupplicant*[3] while the PANA client has been implemented from scratch. The EAP-TLS method was selected as an authentication method between the EAP client and the EAP server.

IPsec Security Associations to secure Mobile IPv6 signaling are established thanks to **racoon** application implementing IKEv1. We used a patched version of **racoon** (by Francis Dupont (Point6/CELAR)). The reason is that the original version of the *IPsec-tools* project is unable to setup correct IPsec SAs for Mobile IPv6 when MN is not in its home domain.

The PANA client receives from the PAA the MN's HoA and the HA address in corresponding AVPs in the PANA-Bind-Request message. After receiving the PANA-Bind-Request message, the PaC launches a shell script that first configures **racoon**, IPsec security policy database, and Mobile IPv6 with those HoA and HA addresses, and second executes **racoon** and Mobile IPv6 daemons.

5.4 Access Router/PAA/AAA Client

The PAA located in host B receives EAP messages from A and forwards them to the AAA client using a UNIX socket. The AAA client is a Diameter EAP client that relies on the WIDEDiameter library. The latter library was developed during the Nautilus6 project and implements the Diameter Base Protocol [17].

[1] www.FreeBSD.org
[2] http://www.mobileip.jp
[3] http://open1x.sourceforge.net

5.5 AAA Server/EAP Server/Home Agent

Host C supports an EAP server, a Diameter EAP server, IPsec components (IKE, AH and ESP), and a HA. SHISA for Mobile IPv6 and HA support was installed as well as the **racoon** version from Francis Dupont.

The Diameter EAP server relies on the WIDEDiameter library. It communicates with the EAP server thanks to a local UNIX socket in order to authenticate the EAP client within the MN. As soon as the authentication is successful, the Diameter EAP server sends the HA address and the HoA to the MN. The assignment is done according to the identity of the MN and a predefined users' database. A shell script is then launched in order to configure **racoon** and IPsec policy and to execute **racoon**.

5.6 Tests and Results

The implementation of this proposal succeeds. It was carried out in several steps.

First of all we tested separately each one of the protocols to make sure that they worked well. Then a modular approach was employed to test if the MN receives correctly the HoA and the HA addresses: on the one hand the AAA server must deliver them correctly to the AAA client and so to the PAA, on the other hand the PAA must deliver them correctly to the MN.

Besides we also made sure that the PSK calculated by the AAA server and the MN were identical and correct. Once all these tests were positive, racoon and MIPv6 were launched automatically by PaC and AAAH server using Shell scripts. The MN and HA were checked to configure their SA and start their MIPv6 exchanges correctly.

Due to some limitations of the racoon implementation, it was not possible to lead some tests with multiple Mobile Nodes.

However tests done with only one Mobile Node have shown that the average time necessary to the MN to start using Mobile IPv6 is about 8.4 s: 0.04 s for PANA procedure, 3.8 s between the end of PANA procedure and the beginning of IKE procedure, 2.2 s for IKE procedure, 1.3 s between the end of IKE procedure and the beginning of BU/BA procedure, and 0.8 s for BU/BA procedure. These measurements were realized on a platform composed of three computers with processors'speed of about 1 GHz, memory of 512 Mo, and 100 Mbit/s links.

It would have been interesting to perform similar measurements on the same platform using DHCPv6 approach. Unfortunately no implementation of this approach is currently available.

By the way, it is important to notice, as the bootstrapping is done when the MN is switch on, the bootstrapping time is not critical as well as mobility mechanisms for handovers.

6 Conclusion

Deploying a new protocol is a challenging task for Internet Service Providers. In the Mobile IPv6 case, ISPs must deploy Home Agents inside their networks and

customers need equipments implementing the protocol. Moreover, as explained in this article, it is necessary to have a scalable way to dynamically assign some Mobile IPv6 specific parameters to customers' devices.

Our proposal provides a way to achieve that goal by slightly modifying the PANA protocol which is under standardization process at the IETF. This approach avoids additional DHCPv6 exchanges and is well optimized with a close integration to the network access authentication.

Acknowledgements

We would like to thank the Nautilus6 project[4] which provides us the Diameter Base Protocol implementation and Francis Dupont for his patch to **racoon**.

We also would like to thank Fabien Allard (France Telecom R&D) for having installed our implementation and performed some tests on a different platform.

References

1. D. Johnson, C. Perkins, and J. Arkko. Mobility Support in IPv6. RFC 3775, June 2004.
2. J. Arkko, V. Devarapalli, and F. Dupont. Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents. RFC 3776, July 2003.
3. A. Patel, K. Leung, M. Khalil, H. Akhtar, and K. Chowdhury. Authentication Protocol for Mobile IPv6. RFC 4285, January 2006.
4. A. Patel and G. Giaretta. Problem Statement for Bootstrapping Mobile IPv6. RFC 4640, September 2006.
5. C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306, December 2005.
6. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). RFC 3748, June 2004.
7. G. Giaretta, J. Kempf, and V. Devarapalli. Mobile IPv6 bootstrapping in split scenario. draft-ietf-mip6-bootstrapping-split-03, October 2006.
8. K. Chowdhury and A. Yegin. Mip6-bootstrapping via DHCPv6 for the Integrated Scenario. draft-ietf-mip6-bootstrapping-integrated-dhc-01, June 2006.
9. R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315, July 2003.
10. D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig, and A. Yegin. Protocol for Carrying Authentication for Network Access. draft-ietf-pana-pana-12, August 2006. Work in progress.
11. C. Perkins. IP Mobility Support for IPv4. RFC 3344, August 2002.
12. R. Moskowitz and P. Nikander. Host Identity Protocol (HIP) Architecture. RFC 4423, May 2006.
13. J. Korhonen, J. Bournelle, H. Tschofenig, C. Perkins, and K. Chowdhury. The NAS - HAAA Interface for MIPv6 Bootstrapping. draft-ietf-dime-mip6-integrated-01, June 2006.

[4] http://www.nautilus6.org

14. K. Chowdbury and A. Liora. RADIUS Attributes for Mobile IPv6 bootstrapping. draft-chowdbury-mip6-bootstrapp-radius-01.txt, October 2004.
15. J. Bournelle, M. Laurent-Maknavicius, and J-M. Combes. Using PANA in the Mobile IPv6 Integrated Case. draft-bournelle-pana-mip6-01, June 2006.
16. D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409, November 1998.
17. P. Calhoun, J. Arrko, E. Guttman, G. Zorn, and J. Loughney. Diameter Base Protocol. RFC 3588, September 2003.