IKEv2-based Home Agent Assignment in Mobile IPv6/NEMO Bootstrapping
draft-dupont-ikev2-haassign-02.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 4, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document specifies how to use IKEv2 for Home Agent assignment in Mobile IPv6 or NEMO bootstrapping. It uses IPv6 anycast addresses and should not introduce new security issues.
1. Introduction

Home Agent (HA) assignment is an improvement over HA discovery: in place of giving a list of possible HA addresses, this procedure gives the HA to use in a way controlled by the Mobile Service Provider, for (initial) load balancing, fail-over or DoS avoidance.

IKEv2 [RFC4306] is the tool of choice in bootstrapping scenarios because not only it established the needed Security Associations but it can allocate home Addresses, authenticate the Mobile Node (MN) using EAP [RFC2284], etc [IKEv2-MIPv6]. The only function it did not support is the HA assignment.

This document addresses both Mobile IPv6 [RFC3775] and NEMO [RFC3963] cases, the second likely with another IPv6 subnet anycast address.

The goal of the document is to provide HA assignment support using an IKEv2 initial message sent to an IPv6 anycast destination address without introduction of new security issues.

This document could use the standard keywords [BCP14] to indicate requirement levels.

2. The proposal

In the IKEv2 exchanges, the MN takes the initiator role and the HA the responder role. The MN takes parameters from its configuration, followed or not by a discovery phase. The HA address is a recognizable IPv6 anycast address. So:

1. the MN sends an IKE_SA_INIT request to the HA anycast address
2. the anycast receiver forwards the request to the "best" HA
3. the HA answers using its own address as the source address and includes an "under attack" cookie in its replies
4. the MN notes the HA own address and use it in subsequent messages, the MN retries the IKE_SA_INIT request with the cookie to the HA own address

The standard IKEv2 procedure follows as usual. The following figure illustrates the initial exchanges:
Figure 1: Initial exchanges

The proposal can be used in any environment, including Mobile IPv6 and NEMO, as soon as a recognizable IPv6 anycast address is assigned to the provided service (cf. IANA (Section 3)).

The term "recognizable IPv6 anycast address" means an IPv6 anycast address [RFC3513] which is recognizable as an IPv6 anycast address by the initiator. This includes, but not exclusively, addresses in the subnet anycast address format defined by [RFC2526].

3. IANA Considerations

Mobile IPv6 defines an IPv6 subnet anycast address [RFC2526] (value decimal=126 / hexa=7E). In the case Mobile IPv6 and NEMO services are not provided by the same HAs, a second IPv6 subnet anycast address has to be assigned by IANA for NEMO HAs.

4. Security Considerations

As the anycast address can be well known, the cookie-based defense against DoS ([RFC4306] section 2.6) is used by default. Another advantage is the whole IKE_SA_INIT and IKE_AUTH exchanges are
performed using the "right" addresses so the impact of the proposal on IKEv2 implementations can be kept minimal.

As in the standard IKEv2 ([RFC4306] section 2.4 4th paragraph) the initiator has to reject cryptographically invalid fake IKE_SA_INIT replies so there is no new attack against the initiator side.

5. Acknowledgments

The initial idea was in a Kilian Weniger’s message about HA assignment. Jean-Michel Combes, speaking for a Mobile Service Provider, insisted to improve the current HA discovery to HA assignment. Kero Kivinen checked whether the proposal introduces new security issue and whether it is reasonably easy to implement, and proposed the figure for initial exchanges.

6. References

6.1. Normative References


6.2. Informative References


Appendix A. Possible Enhancements

The cookie phase is not strictly necessary so it is only RECOMMENDED. Note that one of the main reasons to provide assignment in place of discovery, i.e., perform the server selection by the network in place of the client, is to protect servers against denial of service attacks, so the cost of always using a cookie is in fact low.

The mechanism can be used for other contexts than Mobile IPv6 and NEMO, for instance as a general Security Gateway assignment mechanism. Instead of pre-configuring a well-known anycast addresses on the client, the anycast address can also be discovered prior to sending the IKE_SA_INIT, e.g., with DNS. This allows for more flexibility, i.e., the operator can change the anycast address anytime and it can allocate different anycast addresses to different services. And this simplifies the IANA considerations.

The protocols used between the Home Agents, both to forward the initial request and to select the real server, are not described in this document. They are currently left to the implementor’s choice and can become the object of another document if needed.

Authors’ Addresses

Francis Dupont (editor)
CELAR
Email: Francis.Dupont@fdupont.fr

Kilian Weniger
Panasonic R&D Center Germany
Monzastr. 4c
Langen 63225
Germany

Phone: +49 6103 766 137
Email: kilian.weniger@eu.panasonic.com