Mobility Extensions for IPv6 (Mext)
Internet-Draft
Intended status: Standards Track
Expires: September 9, 2009

W. Haddad
F. Dupont
ISC

March 8, 2009

Enabling an Enhanced Care-of Address Reachability Test for the Home Agent
draft-haddad-mext-enhanced-reachability-test-03

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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 September 9, 2009.

Abstract

This memo aims to improve Mobile IPv6 protocol security by enabling an enhanced care-of address rechability test for the home agent. The main goals are to discourage a rogue mobile node from misleading its home agent to flood a targeted foreign network and to empower the latter to thwart this type of attack if launched at a later stage.

Table of Contents

1. Introduction

Mobile IPv6 protocol (described in [MIPv6]) describes two different modes for handling data packet exchange when the mobile node (MN) is located in a foreign network. These two modes, namely the bidirectional tunneling (BT) and route optimization (RO), have two commonalities. The first one is the mechanism used to update the HA after each IP handoff and requires the MN to send a binding update (BU) message to its HA immediately after configuring a care-of address (CoA). A second commonality is the HA's reaction upon receiving a valid BU message and can be described as a blind trust in the MN claim(s) regarding its new CoA(s). The common consequence is that the HA will always tunnel data packets to the MN's new location without conducting any reachability test on the new claimed CoA.

This memo aims first and foremost to avoid the potential consequences of lack of CoA reachability test on the HA side. For this purpose, it introduces an enhanced and seamless CoA test which makes launching a network flooding attack complicated enough to discourage a rogue MN from misleading its HA to flood a particular target. In addition, it empowers the targeted network to thwart such attack if launched at a later stage.

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 [TERM].

3. Goals and Assumptions

The suggested work is motivated by two main goals. An explicit goal is to improve MIPv6 overall security without increasing the signaling message load on the MN. For this purpose, the key exchange in the proposed mechanism is performed between the MN's HA and the new AR. It should be noted here that repeating the same CoA reachability test as the one which is periodically performed between the MN and its CN(s), i.e., as part of the return routability procedure, will result in a significant increase in the amount of signaling messages on the MN side as it needs also to be repeated periodically in order to be efficient.

The resulting improvement from the proposed mechanism should also benefit other protocols which have been designed around MIPv6, e.g., network mobility protocol (described in [NEMO]). Another goal is to strengthen the network's ability to thwart network flooding attack launched via the MN's HA by improving the network protective means, in the same way as has already been suggested in the network flooding defense mechanism (described in [NFD]) for the enhanced route optimization (described in [ERO]).

Another implicit goal is to provide yet another strong incentive to deploy the secure neighbor discovery protocol (described in [SeND]), as the proposed mechanism assumes that SeND is deployed. This means that the MN is CGA enabled (as described in [CGA]) and is able to exploit all protective features provided by SeND on the link.

4. Proposed Mechanism

In order to address the issues and uncertainties described earlier, we introduce in the following an enhanced secure and seamless CoA reachability test which is triggered by the MN's HA upon receiving a valid BU message from the MN. The suggested reachability test does not directly involve the MN and does not affect the HA treatment of the BU message (as described in RFC3775) nor does it increase the overall latency. In fact, the suggested mechanism involves the MN in three ways. The first one is not new as it has already been used in NFD and consists on establishing a 'symbiotic' relationship (SR) with the AR (described in [SRP]). The second requirement put on the MN is to "partially" inform its HA about the new SR related to its claimed CoA, its new AR's IP address, the AR's public key as well as providing the HA a link to the AR's certificate. Clearly, these information will be sent in the BU message and thus, require defining new options. The third and last requirement is to send also the HA's IPv6 address and its public key to the new AR. Again, this information should be sent in new options carried in one message used during a neighbor discovery protocol (described in [NDP]) exchange, e.g., the router solicitation (RtSol) message.

Establishing an SR with the AR requires the MN to incorporate special parameters in order to generate the 128-bit random parameter (RAN(128)) to be used to configure its CGA address. As described in the SRP mechanism, this means that the RAN(128) used together with the MN's public key and other parameters to generate the 64-bit interface identifier (IID) should in turn, be generated from the AR's public key and another "inner" random 128-bit parameter (I_RAND(128)). The MN should then encrypt the I_RAND(128) with the AR's public key and send it to the AR in an NDP message signed with the MN's CGA private key. In addition, the MN MUST also include the HA's IPv6 address and may also provide the HA's public key. These two parameters will be stored by the AR together with the MN's SR and its public key.

On the HA side, the MN must include in the BU message the AR's IPv6 address, its public key and a link to its certificate, i.e., the same as the one obtained by the MN when attaching to the AR link. In addition, the MN must include in an encrypted form a 128-bit parameter derived from hashing RAND(128) and called HRAND(128)).

As mentioned earlier, the design of the suggested CoA reachability test should avoid increasing the latency. For this purpose, it is highly recommended that the HA triggers the CoA reachability test immediately after launching the DAD procedure for the MN's IPv6 home address, following the receipt of a valid BU message. Triggering an enhanced CoA reachability test requires the HA to send a new message

called "Binding Confirm Request (BCR)" to the MN's AR in which, it must insert the MN's new claimed CoA, a nonce and disclose what it knows about the SR established between the MN and its AR by authenticating the message with HRAND(128). In addition, the HA MAY sign the BCR message.

Upon receiving a BCR message, the AR starts first by checking if the queried CoA is stored in its cache memory. Then it fetches the MN's corresponding SR and uses it to validate the HA knowledge by checking the message authenticity. If the HA's public key is available, and only if the authentication is valid, then the AR proceeds to check also the signature. If the authentication is valid (and the signature if it is provided), then the AR should immediately reply by sending a "Binding Confirm (BC)" message in which, it MUST insert the nonce, authenticate it with HRAND(128) and sign it with its private key.

When the HA gets a BC message from the AR, it starts first by checking the nonce then validates the message authenticity. Then it verifies the signature by using the AR's public key already stored in the MN's corresponding entry. It becomes clear by now that the AR's signature is a key feature as it allows the HA to validate the certificate provided by the MN and provides a solid proof to the HA about the AR's role and topological location. Hence, if the signature is valid, then the HA can consider with enough confidence that the MN has indeed visited the AR and exchanged NDP messages with it and an SR has been accepted. Furthermore, it also serves as an indication to the HA that the AR is now empowered to repel any malicious behavior that can emanate from the MN, e.g., launching a flooding attack at a later stage. It follows that the CoA reachability test does not need to be repeated periodically.

After completing a successful reachability test, i.e., performed in parallel with the DAD procedure in the home network, the HA starts tunneling data packets to the MN's new CoA. As already mentioned, the presence of the SR between the MN and its AR will prevent the MN from moving away at some point, and launching a flooding attack by keeping sending acknowledgment messages to the CN, e.g., using another interface. In fact, in case such an attack is launched, the AR will quickly detect the MN's absence on the link and securely request the HA to halt the data packets flow to the MN's CoA. Note that in our context, making a secure request to the HA implies that the AR MUST send the SR established by the MN without encryption and must sign the message with its private key. This also means that processing such request on the HA side means that it has to check first if the SR is valid by hashing it and comparing the hash to the corresponding HRAND(128).

5. New Options and Messages Formats

TBD

6. Security Considerations

This document introduces an enhanced and seamless CoA reachability test especially designed to be used by the HA in order to check the MN's topological location and compare it to the claimed CoA. In fact, the proposed mechanism enables to address uncertainties surrounding a potential network flooding threat in MIPv6 protocol as well as in its derivative(s). Consequently, the main goal is to improve the security in MIPv6 in a way which does not directly involve the MN and does not require a periodic exchange of signaling messages.

The proposed mechanism is inspired from the NFD mechanism which is tightly based on the SR concept to enable replacing the periodic CoA reachability test on the CN side. In other words, the presence of an SR does not require adding new parameters in order to secure the exchange between the HA and the AR, although this is possible.

Our suggested protocol also assumes that the HA is always interested in validating the MN's claimed CoA prior to any data traffic redirection to the new claimed CoA. Such assumption severely limits the MN's manoeuvrability room for bypassing such test since the absence of any information regarding the AR and SR in the BU message will lead the HA to test the MN's CoA reachability using a state cookie as described in [CTSC], i.e., by asking the MN directly upon receiving a valid BU message. In such scenario, if the MN has established an SR with the AR but avoided disclosing it to its HA, then it will have to answer the reachability test by itself which implies sending an additional mobility signaling message. Otherwise, i.e., in the absence of an SR, the AR won't forward the message sent by the HA to its final destination in which case, the MN won't be able to answer the reachability test nor to get its data traffic. This also means that the MN won't be able to launch any attack as it will be practically considered by the AR as non-existing on its link.

7. References

7.1. Normative References

[CGA] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3792, March 2005.

[ERO] Vogt, C., Arkko, J., and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", RFC 4866, June 2006.

[MIPv6] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support for IPv6", RFC 3775, June 2004.

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

[NEMO] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[SeND] Arkko, J., Kempf, J., Sommerfield, B., Zill, B., and P. Nikander, "Secure Neighbor Discovery (SeND)", RFC 3971, March 2005.

[TERM] Bradner, S., "Key Words for Use in RFCs to Indicate Requirement Levels", RFC 2119, BCP , March 1997.

7.2. Informative References

[CTSC] Dupont, F. and J. Combes, "Care-of Address Test for MIPv6 using a State Cookie", Internet Draft, draft-dupont-mipv6-rrcookie-05.txt, November 2007.

[NFD] Haddad, W. and M. Naslund, "On Using 'Symbiotic Relationship' to Repel Network Flooding Attack", Internet Draft, draft-haddad-mipshop-netflood-defense-02.txt, October 2008.

[SRP] Haddad, W. and M. Naslund, "On Secure Neighbor Discovery Proxying Using 'Symbiotic' Relationship", Internet Draft, draft-haddad-csi-symbiotic-sendproxy-00.txt, October 2008.

Authors' Addresses

Wassim Haddad
US

Phone: +1 646 2568041
Email: wmhaddad@gmail.com

Francis Dupont
ISC

Email: Francis.Dupont@fdupont.fr