Internet Engineering Task Force (IETF)
Request for Comments: 6496
Category: Experimental
ISSN: 2070-1721

S. Krishnan
Ericsson
J. Laganier
Juniper Networks
M. Bonola
Rome Tor Vergata University
A. Garcia-Martinez
UC3M

February 2012

Secure Proxy ND Support for SEcure Neighbor Discovery (SEND)

Abstract

SEcure Neighbor Discovery (SEND) specifies a method for securing Neighbor Discovery (ND) signaling against specific threats. As defined today, SEND assumes that the node sending an ND message is the owner of the address from which the message is sent and/or possesses a key that authorizes the node to act as a router, so that it is in possession of the private key or keys used to generate the digital signature on each message. This means that the Proxy ND signaling performed by nodes that do not possess knowledge of the address owner's private key and/or knowledge of a router's key cannot be secured using SEND. This document extends the current SEND specification in order to secure Proxy ND operation.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6496.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

SEcure Neighbor Discovery (SEND) [RFC3971] specifies a method for securing Neighbor Discovery (ND) signaling [RFC4861] against specific threats [RFC3756]. As defined today, SEND assumes that the node sending an ND message is the owner of the address from which the message is sent and/or possesses a key that authorizes the node to

act as a router, so that it is in possession of the private key or keys used to generate the digital signature on each message. This means that the Proxy ND signaling performed by nodes that do not possess knowledge of the address owner's private key and/or knowledge of a router's key cannot be secured using SEND.

This document extends the current SEND specification with support for Proxy ND. From this point on, we refer to such an extension as "Secure Proxy ND Support for SEND".

2. Requirements Notation

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 [RFC2119].

3. Terminology

Secure ND Proxy

A node acting on behalf of another node and authorized to secure a Neighbor Discovery Protocol (NDP) message without knowing the private key related to the source address of the other node or the key related to the router authorization.

Proxied IPv6 address

An IPv6 address that does not belong to the Secure ND Proxy and for which the Secure ND Proxy is performing advertisements.

Non-SEND node

An IPv6 node that does not implement the SEND [RFC3971] specification but uses the ND protocol defined in [RFC4861] and [RFC4862], without additional security.

RFC 3971 node

An IPv6 node that does not implement the specification defined in this document for Secure Proxy ND support but uses the SEND specification as defined in [RFC3971].

Secure Proxy ND (SPND) node

An IPv6 node that receives and validates messages according to the specification defined in this document for Secure Proxy ND support.

Translated NDP message

An NDP message issued by a Secure ND Proxy as a result of a received NDP message originated by the owner of the address or originated by another node acting on behalf of the owner of the address.

Synthetic NDP message

An NDP message issued by a Secure ND Proxy that is not the result of a received NDP message.

4. Secure Proxy ND Overview

The original SEND specification [RFC3971] has implicitly assumed that only the node sending an ND message is the owner of the address from which the message is sent. This assumption does not allow proxying of ND messages, since the advertiser is required to generate a valid RSA Signature option, which in turn requires possession of the public-private key pair that was used to generate a Cryptographically Generated Address (CGA), or that was associated to a router certificate.

To be able to separate the roles of owner and advertiser, the following extensions to the SEND protocol are defined:

- A Secure Proxy ND certificate, which is a certificate authorizing an entity to act as an ND proxy. It is an X.509v3 certificate in which the purpose for which the certificate is issued has been specified explicitly, as described in a companion document [RFC6494]. Briefly, Secure Proxy ND certificates include one or more KeyPurposeId values that can be used for authorizing proxies to sign Router Advertisement (RA) and Redirect messages, or to sign Neighbor Advertisement (NA), Neighbor Solicitation (NS), or Router Solicitation (RS) messages on behalf of other nodes. The inclusion of this value allows the certificate owner to perform proxying of SEND messages for a range of addresses indicated in the same certificate. This certificate can be exchanged through the Authorization Delegation Discovery process defined in [RFC3971].

- A new Neighbor Discovery option called the Proxy Signature (PS) option. This option contains the hash value of the public key of the proxy, and the digital signature of the SEND message computed with the private key of the proxy. The hash of the public key of the proxy is computed over the public key contained in the Secure

Proxy ND certificate. When an ND message contains a PS option, it MUST NOT contain CGA or RSA Signature options. The PS option MUST be appended to any NDP message (NA, NS, RS, RA, and Redirect) to secure it.

- A modification of the SEND processing rules for all ND messages: NA, NS, RS, RA, and Redirect. When any of these messages containing a PS option is validated, it is considered secure.

These extensions are applied in the following way:

- A Secure ND Proxy that proxies ND messages on behalf of a node can use the PS option to protect the proxied messages. This Secure ND Proxy becomes part of the trusted infrastructure just like a SEND router.

- The messages to be secured with the PS option are built according to [RFC4861] if they are synthesized by the Secure ND Proxy, or they result from the processing rules defined in [RFC4389] if they are translated ND messages.

- In order to allow nodes to successfully validate secured proxied messages, the nodes MUST be aware of the Secure Proxy ND certificate (in the format described in [RFC6494]) and MUST apply the modified processing rules specified in this document. We call these nodes 'SPND nodes'. Note that the rules for generating ND messages in SPND nodes do not change, so these nodes behave as defined in [RFC3971] when they send ND messages.

- To allow SPND nodes to know the certification path required to validate the public key of the proxy, devices responding to CPS (Certification Path Solicitation) messages with CPA (Certification Path Advertisement) messages as defined in Section 6 of the SEND specification [RFC3971] are extended to support the certificate format specified in [RFC6494], and are configured with the appropriate certification path.

5. Secure Proxy ND Specification

A Secure ND Proxy performs all the operations described in the SEND specification [RFC3971] with the addition of new processing rules to ensure that the receiving node can identify an authorized proxy generating a translated or synthetic SEND message for a proxied address.

This is accomplished by signing the message with a private key of the authorized Secure ND Proxy. The signature of the Secure ND Proxy is included in a new option called the PS option. The signature is

performed over all the Neighbor Discovery Protocol (NDP) options present in the message, and the PS option is appended as the last option in the message.

5.1. Proxy Signature Option

The Proxy Signature option allows signatures based on public keys to be attached to NDP messages. The format of the PS option is described in the following diagram:

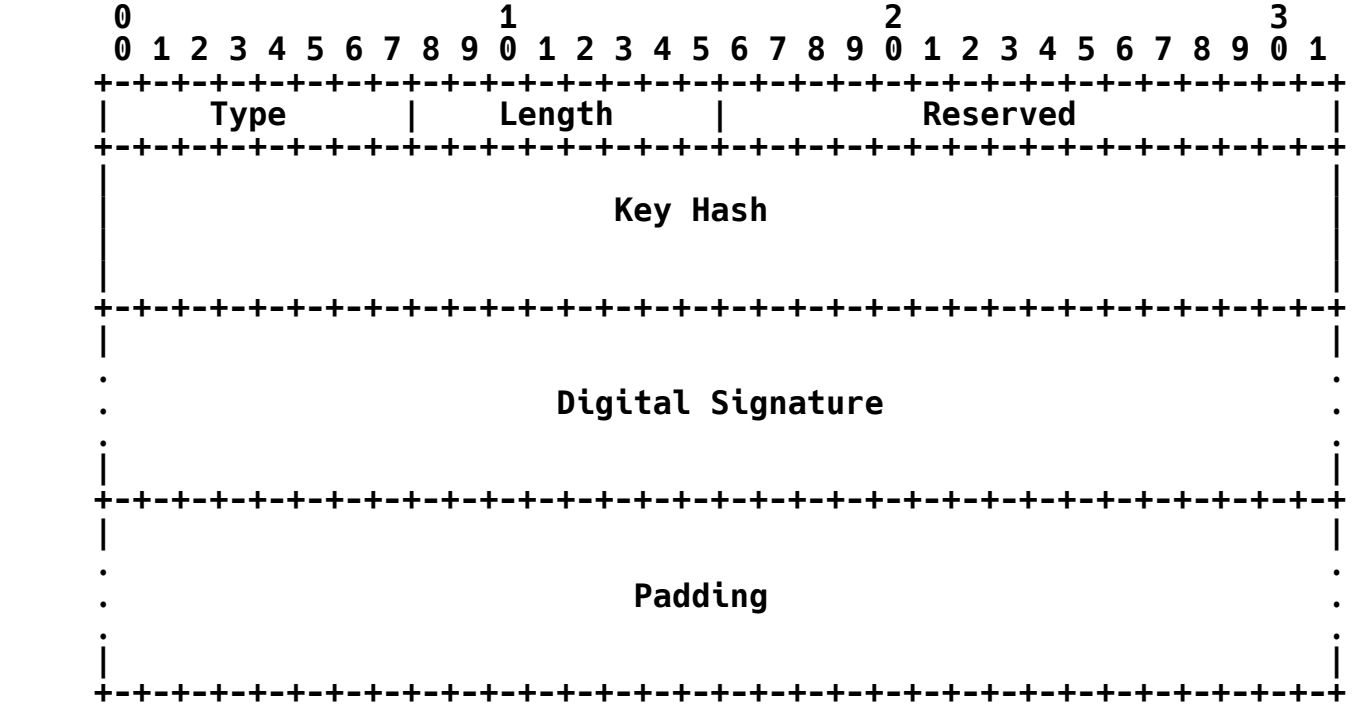

Figure 1: PS Option Layout

Type

32

Length

The length of the option (including the Type, Length, Reserved, Key Hash, Digital Signature, and Padding fields) in units of 8 octets.

Reserved

A 16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Key Hash

A 128-bit field containing the most significant (leftmost) 128 bits of a SHA-1 [SHA1] hash of the public key used for constructing the signature. Its purpose is to associate the signature to a particular key known by the receiver. Such a key MUST be the same one within the corresponding Secure Proxy ND certificate.

Digital Signature

A variable-length field containing a PKCS#1 v1.5 signature, constructed by using the sender's private key over the following sequence of octets:

1. The 128-bit CGA Message Type tag [RFC3972] value for Secure Proxy ND, 0x09F5 2BE5 3B62 4C76 CB96 4E7F CDC9 2804. (The tag value has been generated randomly by the editor of this specification.)

2. The 128-bit Source Address field from the IP header.

3. The 128-bit Destination Address field from the IP header.

4. The 8-bit Type, 8-bit Code, and 16-bit Checksum fields from the ICMP header.

5. The NDP message header, starting from the octet after the ICMP Checksum field and continuing up to, but not including, NDP options.

6. All NDP options preceding the Proxy Signature option.

The signature value is computed with the RSASSA-PKCS1-v1_5 algorithm and SHA-1 hash, as defined in [RSA]. This field starts after the Key Hash field. The length of the Digital Signature field is determined by the ASN.1 BER coding of the PKCS#1 v1.5 signature.

Padding

This variable-length field contains padding. The length of the padding field is determined by the length of the Proxy Signature option minus the length of the other fields.

5.2. Modified SEND Processing Rules

This specification modifies the sender and receiver processing rules defined in the SEND specification [RFC3971].

5.2.1. Processing Rules for Senders

A Secure ND Proxy MUST NOT use a key to sign NDP message types that do not correspond to the authorization granted to the considered key. NA, NS, and RS messages MUST be signed with a key corresponding to a Secure Proxy ND certificate with a KeyPurposeId value [RFC6494] of id-kp-sendProxiedOwner, and the source addresses of the messages MUST be encompassed in the prefix associated to the certificate. RA and Redirect messages MUST be signed with a key corresponding to a Secure Proxy ND certificate with a KeyPurposeId value of id-kp-sendProxiedRouter. The prefix included in the RA message for on-link determination and/or stateless address autoconfiguration, and the Target Address of the Redirect message, MUST be encompassed in the prefix associated to that certificate.

A secured NDP message sent by a Secure ND Proxy for a proxied address MUST contain a PS option and MUST NOT contain either CGA or RSA Signature options. Section 7 discusses in which cases an NDP message has to be secured in a scenario including non-SEND nodes.

The input of this process is a message obtained in either of the following ways:

a. If the Secure ND Proxy generates synthetic SEND messages for a proxied address, the message MUST be constructed as described in the Neighbor Discovery for IP version 6 specification [RFC4861].

b. If the Secure ND Proxy translates secured messages, first the authenticity of the intercepted message MUST be verified. If the intercepted message is a SEND message, it MUST be validated as specified in Section 5 of the SEND specification [RFC3971]. If the intercepted message contains a PS option, the authenticity of the message MUST be verified as detailed in Section 5.2.2 of this specification. After validation, the CGA, RSA, or PS options of the original message MUST be removed. Then, the message to be translated MUST be processed according to the ND Proxy specification [RFC4389]. In this way, it is determined whether

the message received should be proxied or not; the proxy interface status is updated if needed, the outgoing interface is determined, the link-layer header and the link-layer address within the payload are modified if required, etc.

A Secure ND Proxy then modifies the input message as follows:

1. Timestamp and Nonce options MUST be included according to the rules specified in SEND [RFC3971]. The value in the Timestamp option MUST be generated by the proxy. If the proxy is translating a message that includes a nonce, the Nonce value in the proxied message MUST be the same as in the intercepted message. If the proxy is synthesizing a solicitation message, the Nonce value MUST be generated by the proxy. If the proxy is synthesizing an advertisement message, the Nonce value MUST correspond to the solicitation message to which the proxy is responding.

2. The Proxy Signature option MUST be added as the last option in the message.

3. The data MUST be signed as explained in Section 5.1.

5.2.2. Processing Rules for Receivers

Any SEND message without a Proxy Signature option MUST be treated as specified in the SEND specification [RFC3971].

A SEND message including a Proxy Signature option MUST be processed as specified below:

1. The receiver MUST ignore any RSA and CGA options, as well as any options that might come after the first PS option. The options are ignored for both signature verification and NDP processing purposes.

2. The Key Hash field MUST indicate the use of a known public key. A valid certification path (see [RFC6494] Section 9) between the receiver's trust anchor and the sender's public key MUST be known. The Secure Proxy ND X.509v3 certificate MUST contain an extended key usage extension including the appropriate KeyPurposeId value and prefix for the message to validate:

   * For RA messages, a KeyPurposeId value of id-kp-sendProxiedRouter MUST exist for the certificate, and the prefix included in the RA message for on-link determination and/or stateless address autoconfiguration MUST be encompassed in the prefix associated to that certificate.

* For Redirect messages, a KeyPurposeId value of id-kp-sendProxiedRouter MUST exist for the certificate, and the prefix included in the Target Address of the Redirect message MUST be encompassed in the prefix associated to that certificate.

* For NA, NS, and RS messages, a KeyPurposeId value of id-kp-sendProxiedOwner MUST exist for the certificate, and the source addresses of the messages MUST be encompassed in the prefix associated to the certificate.

If any of these tests fail, the verification fails.

3. The Digital Signature field MUST have correct encoding; otherwise, the verification of the message including the PS option fails.

4. The Digital Signature verification MUST show that the signature has been calculated as specified in Section 5.1; otherwise, the verification of the message including the PS option fails.

5. The Nonce option MUST be processed as specified in [RFC3971] Section 5.3.4, except for replacing 'RSA Signature option' with 'PS option'; if these tests fail, the verification of the message including the PS option fails.

6. The Timestamp option MUST be processed as specified in [RFC3971] Section 5.3.4, except for replacing 'RSA Signature option' with 'PS option'. If these tests fail, the verification of the message including the PS option fails. The receiver SHOULD store the peer-related timing information specified in [RFC3971] Sections 5.3.4.1 and 5.3.4.2 (RDlast, TSlast) separately for each different proxy (which could be identified by the different Key Hash values of the proxied message) and separately from the timing information associated to the IP address of a node for which the message is proxied. In this way, a message received for the first time from a proxy (i.e., for which there is no information stored in the cache) for which the Timestamp option is checked SHOULD be checked as a message received from a new peer (as in [RFC3971] Section 5.3.4.2).

7. Messages with the Override bit [RFC4861] set MUST override an existing cache entry regardless of whether it was created as a result of an RSA Signature option or a PS option validation. When the Override bit is not set, the advertisement MUST NOT update a cached link-layer address created securely by means of RSA Signature option or PS option validation.

Messages for which the verification fails MUST be silently discarded if the node has been configured to accept only secured ND messages. The messages MAY be accepted if the host has been configured to accept both secured and unsecured messages but MUST be treated as an unsecured message.

5.3. Proxying Link-Local Addresses

SEND [RFC3971] relies on certificates to prove that routers are authorized to announce a certain prefix. However, Neighbor Discovery [RFC4861] states that routers do not announce the link-local prefix (fe80::/64). Hence, it is not required for a SEND certificate to hold an X.509 extension for IP addresses that authorizes the fe80::/64 prefix. However, some Secure Proxy ND scenarios ([RFC4389], [RFC5213]) impose providing the proxying function for the link-local address of a node. When Secure ND Proxy functionality for a link-local address is required, either a list of link-local addresses, or the fe80::/64 prefix MUST be explicitly authorized to be proxied in the corresponding certificate.

6. Application Scenarios

In this section, we describe three different application scenarios for which Secure Proxy ND support for SEND can be applied. Note that the particular way in which Secure Proxy ND support is applied (which ND messages are proxied, in which direction, how the interaction with non-SEND hosts and RFC 3971 hosts is handled, etc.) largely depends on the particular scenario considered. In the first two scenarios presented below, ND messages are synthesized on behalf of off-link nodes. In the third one, ND messages are translated from the messages received in other interfaces of the proxy.

6.1. Scenario 1: Mobile IPv6

The description of the problems for deploying SEND in this scenario is presented in [RFC5909].

The Mobile IPv6 (MIPv6) protocol [RFC6275] allows a Mobile Node (MN) to move from one link to another while maintaining reachability at a stable address, the so-called MN's Home Address (HoA). When an MN attaches to a foreign network, all the packets sent to the MN's HoA by a Correspondent Node (CN) on the home link or a router are intercepted by the Home Agent (HA) on that home link, encapsulated, and tunneled to the MN's registered Care-of Address (CoA).

To deploy Secure Proxy ND in this scenario, i.e., to secure the HA operation, a Secure Proxy ND certificate with a KeyPurposeId value of id-kp-sendProxiedOwner for the prefix of the home link is required.

The Secure ND Proxy is configured with the private key associated to this certificate. When a NS is intercepted by the HA on the home link, the HA checks whether the Target Address within the NS matches with any of the MN's Home Addresses in the binding cache, and if so, it replies with a Neighbor Advertisement (NA) constructed as described in [RFC4861], containing its own link-layer address (HA_LL) as the Target Link-Layer Address Option (TLLAO). Then, a timestamp (generated by the proxy) and nonce (if appropriate, according to [RFC3971]) MUST be included. Finally, a PS option signing the message MUST be included as the last option of the message.

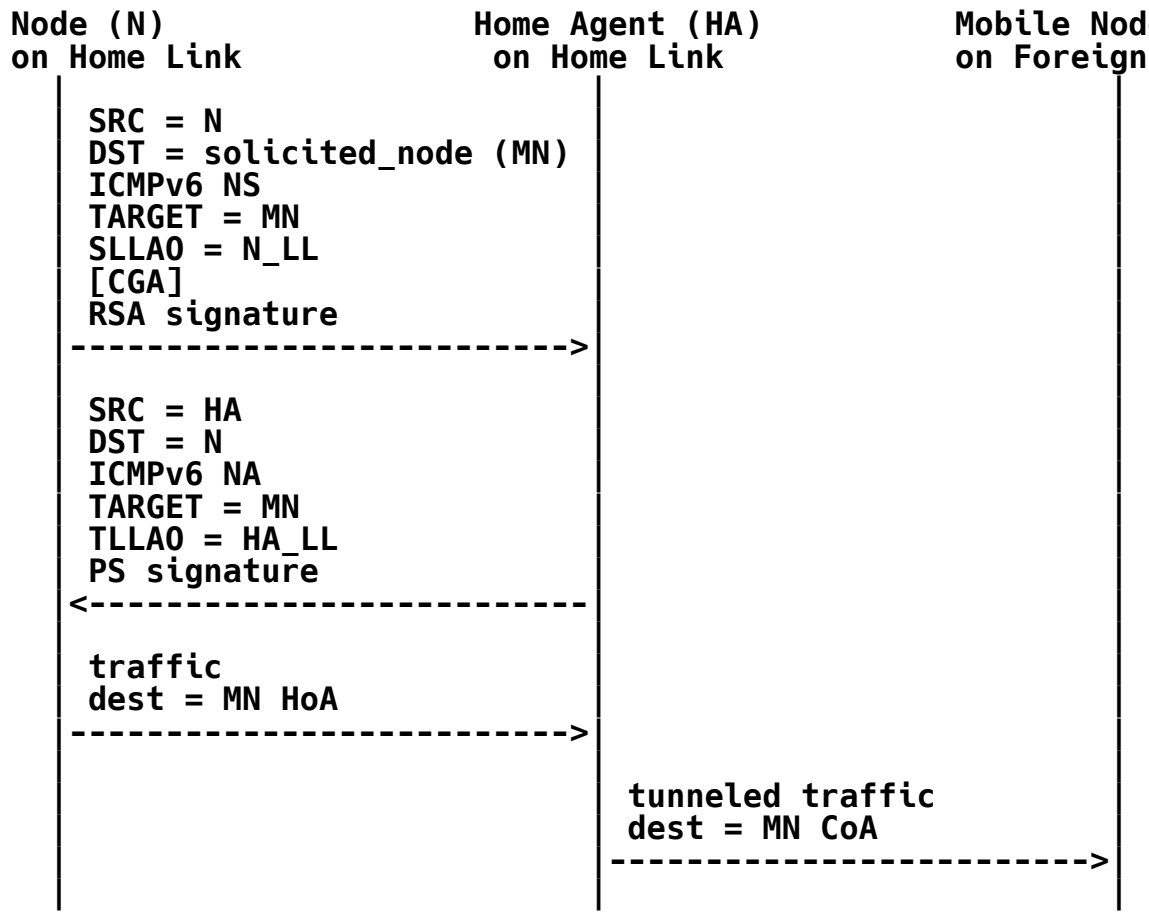

Figure 2: Proxy ND Role of the Home Agent in MIPv6

A node receiving the NA containing the PS option (e.g., the CN in the home link, or a router) MUST apply the rules defined in Section 5.2.2. Note that in this case the Override bit of the NA message is used to control which messages should prevail on each

case: the message generated by the proxy when the MN moves from the home network, or the MN if it comes back to the home link, as defined in the MIPv6 specification [RFC6275].

6.2. Scenario 2: Proxy Mobile IPv6

Proxy Mobile IPv6 [RFC5213] is a network-based mobility management protocol that provides IP mobility management support for MNs without requiring that MNs be involved in the mobility-related signaling. The IP mobility management is totally hidden to the MN in a Proxy Mobile IPv6 domain, and it is performed by two functional entities: the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG).

When the MN connects to a new access link, it sends a multicast Router Solicitation (RS). The MAG on the new access link, upon detecting the MN's attachment, signals the LMA requesting an update of the binding state of the MN (by means of a Proxy Binding Update (PBU)). Once the signaling is completed (it receives a Proxy Binding Ack (PBA)), the MAG replies to the MN with a Router Advertisement (RA) containing the home network prefix(es) that were assigned to that mobility session, making the MN believe it is still on the same link, so the IPv6 address reconfiguration procedure is not triggered (Figure 3).

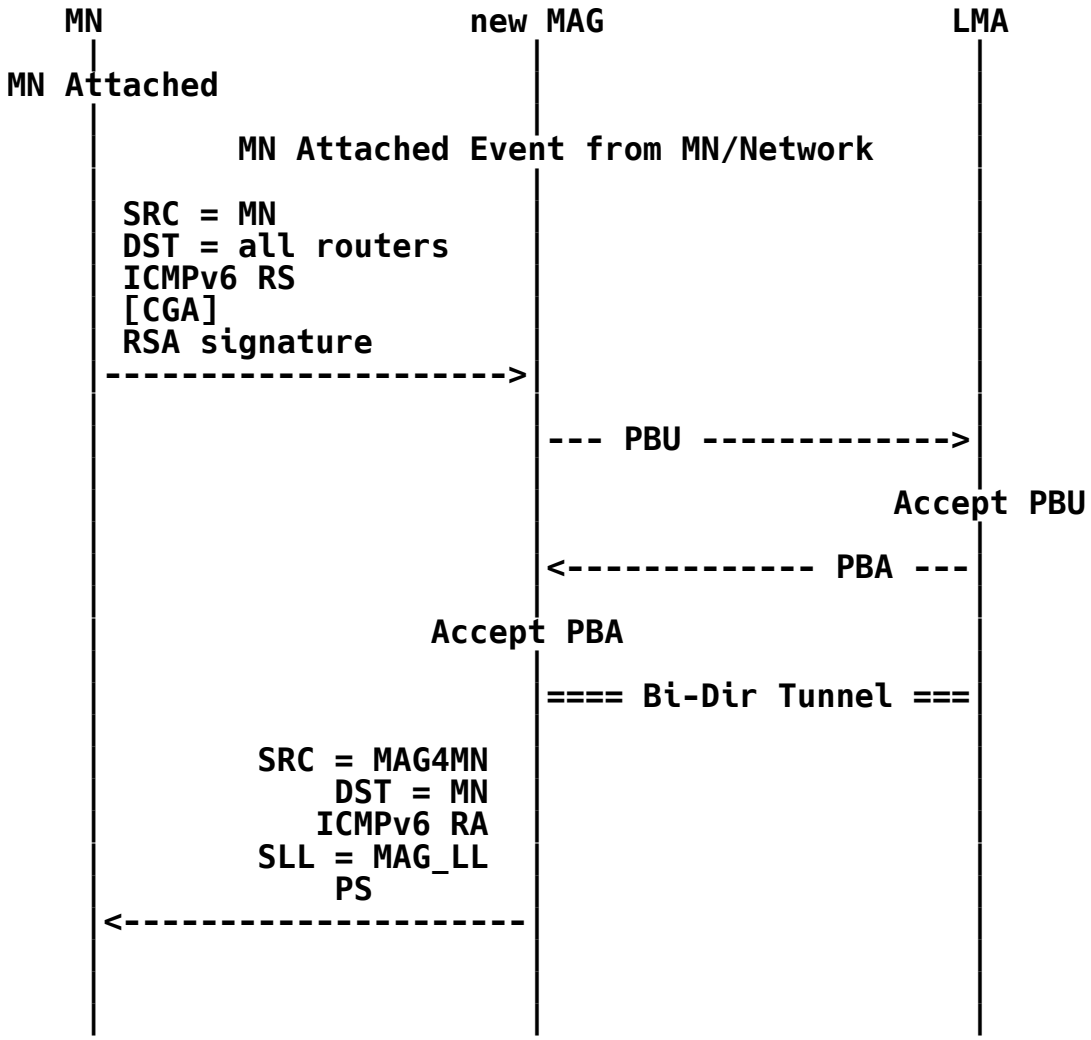

Figure 3: Mobile Node's Handover in PMIPv6

To avoid potential link-local address collisions between the MAG and the MN after a handoff to a new link, the Proxy Mobile IPv6 specification [RFC5213] requires that the MAG's link-local address on the link to which the MN is attached be generated by the LMA when the MN first attaches to a PMIPv6 domain, and be provided to the new MN's serving MAG after each handoff. Thus, from the MN's point of view, the MAG's link-local address remains constant for the duration of that MN's session.

The approach described above and the current SEND specification are incompatible, since sharing the same link-local address on different MAGs would require all MAGs of a PMIPv6 domain to construct the CGA and the RSA Signature option with the same public-private key pair, which is not an acceptable security policy.

Using different public-private key pairs on different MAGs would mean that different MAGs use different CGAs as link-local addresses. Thus, the serving MAG's link-local address would change after each handoff of the MN, which is in contradiction with the way MAG link-local address assignment occurs in a PMIPv6 domain.

To provide SEND protection, each MAG MUST be configured to act as a proxy by means of a certificate associated to the PMIPv6 domain, authorizing each MAG to securely proxy NA and RS messages by means of a KeyPurposeId value of id-kp-sendProxiedOwner. In addition, the certificate MUST also authorize the MAG to advertise prefixes by associating to the same certificate a KeyPurposeId value of id-kp-sendProxiedRouter. Note that the inclusion of multiple KeyPurposeId values is supported by [RFC6494].

When a MAG replies to an RS with an RA, the source address MUST be equal to the MAG link-local address associated to the MN in this PMIPv6 domain, with its own link-layer address as the source link-layer address. Then, a timestamp (generated by the proxy) and nonce (if appropriate, according to [RFC3971]) MUST be included. Finally, a PS option signing the message MUST be included as the last option of the message. This procedure is followed for any other ND message that could be generated by the MAG to the MN.

A node receiving a message from the MAG containing the PS option MUST apply the processing rules defined in Section 5.2.2. Note that unsolicited messages sent by the MAG should be validated by the host according to timestamp values specific to the MAG serving the link, not to any other MAG to which the host has been connected before in other links, according to processing step number 6 of Section 5.2.2.

6.3. Scenario 3: RFC 4389 Neighbor Discovery Proxy

The problems for deploying SEND in this scenario are presented in [RFC5909].

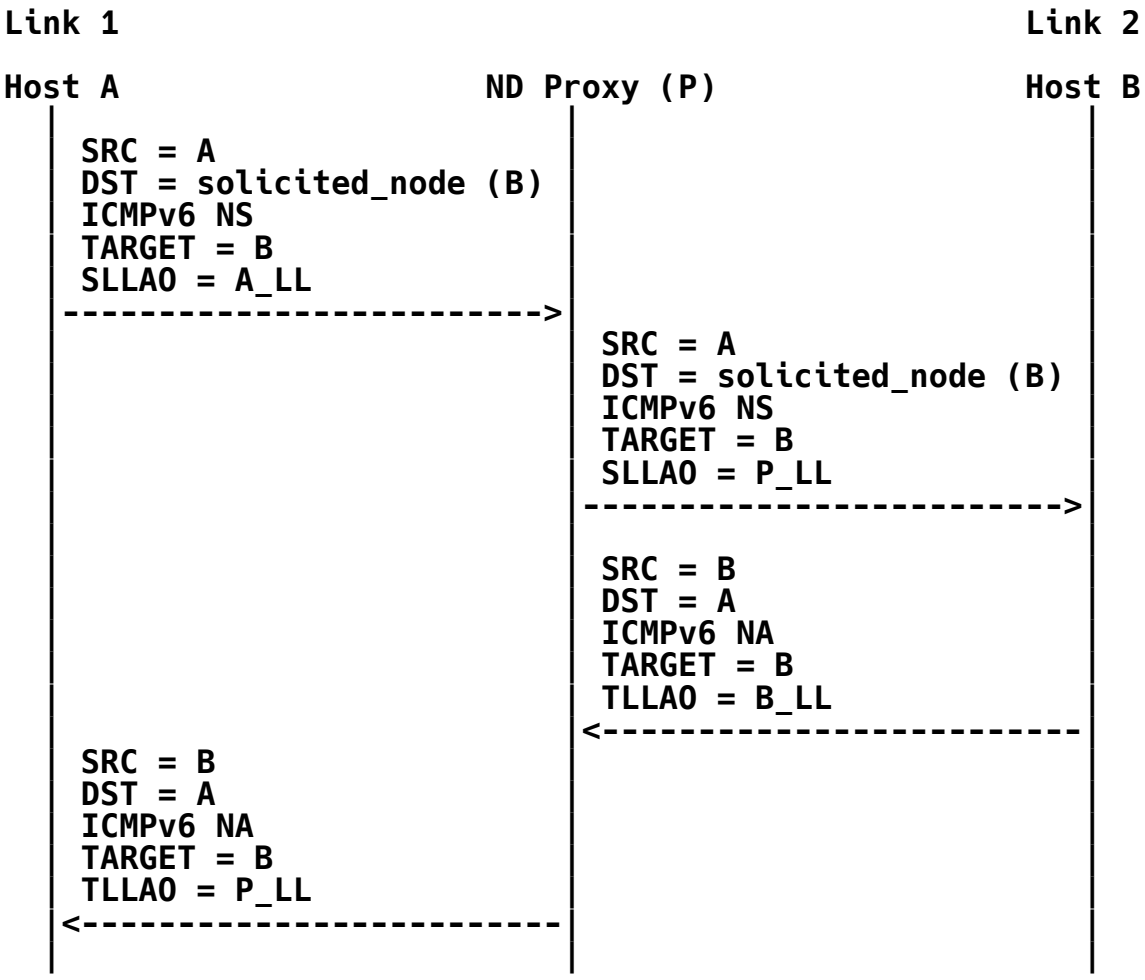

Figure 4: RFC 4389 Neighbor Discovery Proxy Operation

The Neighbor Discovery (ND) Proxy specification [RFC4389] provides a method by which multiple link-layer segments are bridged into a single segment and specifies the IP-layer support that enables bridging under these circumstances.

A Secure ND Proxy MUST parse any IPv6 packet it receives on a proxy interface to check whether it contains one of the following NDP messages: NS, NA, RS, RA, or Redirect. The Secure ND Proxy MUST verify the authenticity of the received ND message, according to [RFC3971], or according to Section 5.2.2 if it contains a PS option.

Then, after removing the CGA, RSA, or PS options, the message to be translated MUST be processed according to the ND Proxy specification [RFC4389]. This includes performing loop prevention checks, determining the outgoing interface for the proxied message, changing the source link-layer address to the address of the outgoing interface, changing source link-layer addresses contained in the payload (that is, in a Source Link-Layer Address Option (SLLAO) or a Target Link-Layer Address Option (TLLAO)), maintaining the destination link-layer address as the address in the neighbor entry corresponding to the destination IPv6 address, setting the P bit for proxied RA messages, etc. Note that besides link-layer addresses and the P bit of a RA, no other field of the received message is changed when proxied by an [RFC4389] proxy.

When any other IPv6 unicast packet is received on a proxy interface, if it is not locally destined, then it is forwarded unchanged (other than using a new link-layer header) to the proxy interface for which the next-hop address appears in the neighbor cache. If no neighbor cache entry is present, the Secure ND Proxy SHOULD queue the packet and initiate a Neighbor Discovery signaling as if the NS message were locally generated.

Note that to be able to sign any NS, NA, RS, RA, or Redirect message, the key used MUST correspond to a certificate with KeyPurposeId values of id-kp-sendProxiedOwner and id-kp-sendProxiedRouter.

In order to deploy this scenario, nodes in proxied segments MUST know the certificate-authorizing proxy operation. To do so, it could be required that at least one device per proxied segment (maybe the proxy itself) be configured to propagate the required certification path to authorize proxy operation by means of a CPS/CPA exchange.

7. Backward Compatibility with RFC 3971 Nodes and Non-SEND Nodes

In this section, we discuss the interaction of Secure ND Proxies and SPND nodes with RFC 3971 nodes and non-SEND nodes. As stated in [RFC3971], network operators may want to run a mixture of nodes accepting secured and unsecured NDP messages at the same time. Secure ND Proxies and SPND nodes SHOULD support the use of secured and unsecured NDP messages at the same time.

7.1. Backward Compatibility with RFC 3971 Nodes

RFC 3971 nodes, i.e., SEND nodes not compliant with the modifications required in Section 5, cannot correctly interpret a PS option received in a proxied ND message. These SEND nodes silently discard the PS option, as specified in [RFC4861] for any unknown option. As

a result, these messages will be treated as unsecured, as described in Section 8 ("Transitions Issues") of the SEND specification [RFC3971].

When RFC 3971 nodes and SPND nodes exchange ND messages (without proxy intervention), in either direction, messages are generated according to the SEND specification [RFC3971], so these nodes interoperate seamlessly.

In the scenarios in which the proxy translates ND messages, the messages to translate can either be originated in an RFC 3971 node or in an SPND node, without interoperability issues (note that the difference between RFC 3971 nodes and SPND nodes only affects the ability to process received NDP messages containing a PS option, not the way they generate messages secured by SEND).

A configuration option MAY exist in a Secure ND Proxy to specify the RFC 3971 nodes to which it is connected, so that the proxied messages sent to these nodes are not processed according to the Secure Proxy ND specification, for performance reasons.

7.2. Backward Compatibility with Non-SEND Nodes

Non-SEND nodes receiving NDP packets silently discard PS options, as specified in [RFC4861] for any unknown option. Therefore, these nodes interpret messages proxied by a Secure ND Proxy as any other ND message.

When non-SEND nodes and SPND nodes exchange ND messages (without proxy intervention), in either direction, the rules specified in Section 8 of [RFC3971] apply.

A Secure ND Proxy SHOULD support the use of secured and unsecured NDP messages at the same time, although it MAY have a configuration that causes proxying to not be performed for unsecured NDP messages. A Secure ND Proxy MAY also have a configuration option whereby it disables secure ND proxying completely. This configuration SHOULD be switched off by default; that is, security is provided by default. In the following paragraphs, we discuss the recommended behavior of the Secure ND Proxy regarding the protection level to provide to proxied messages in a mixed scenario involving SPND/RFC 3971 nodes and non-SEND nodes. In particular, two different situations occur, depending on whether the proxied nodes are RFC 3971 or SPND nodes, or non-SEND nodes.

As a rule of thumb, if the proxied nodes can return to the link in which the proxy operates, the Secure ND Proxy MUST only generate PS options on behalf of nodes with SEND capabilities (i.e., those nodes

that could use SEND to defend their messages if present on the same link as the proxy -- in other words, either RFC 3971 nodes or SPND nodes). This is relevant to allow nodes to prefer secured information over an unsecured one, and to properly execute the Duplicate Address Detection (DAD) procedure, as specified in [RFC3971]. Therefore, in this case, the Secure ND Proxy MUST synthesize/translate messages containing the PS option for SPND and RFC 3971 hosts, and MUST NOT synthesize/translate messages containing the PS option for non-SEND nodes. Note that ND advertisements in response to solicitations generated by a Secure ND Proxy must either be secured or not secured, according to the previous considerations (i.e., according to the nature of the proxied node), and not according to the secure or unsecure nature of the solicitation message.

In order to apply this rule, the Secure ND Proxy needs to know the security capabilities of the proxied node. The way this information is acquired depends on the application scenario, and it is discussed next:

- For scenarios in which ND messages are translated for nodes that can arrive to the link in which the proxy operates, the rule can be easily applied: only for messages validated in the Secure ND Proxy according to the SEND specification [RFC3971], or according to Section 5.2.2 of this specification for messages containing a PS option (which means that another proxy previously checked that the original message was secured), the message MUST be proxied securely by the inclusion of a PS option. Unsecured ND messages could be proxied if unsecured operation is enabled in the proxy, but the message generated by the Secure ND Proxy for the received message MUST NOT include a PS option.

- For scenarios in which ND messages are synthesized on behalf of remote nodes, different considerations should be made according to the particular application scenario.

  * For MIPv6, if the MN can return to the home link, it is required that the proxy know whether the node could use SEND to defend its address or not. A HA including the PS option for proxying a non-SEND MN would make ND messages sent by the proxy be more preferred than an ND message of the non-SEND MN when the MN returns to the home link (even if the proxied messages have the Override bit set to 1). Not using the PS option for an RFC 3971 or SPND MN would make the address in the home link more vulnerable when the MN is away than when it is in the home link, defeating the purpose of the Secure Proxy ND mechanism. Therefore, in this case, the HA MUST know the SEND capabilities

of the MN, MUST use the PS option if the MN is an SPND or RFC 3971 host, and MUST NOT use the PS option for non-SEND hosts.

* For the Proxy Mobile IPv6 scenario, a node moving from a link in which the PS option has been used to protect a link-layer address to a link in which ND messages are not protected by SEND would prevent the MN from acquiring the new information until the cached information expires. However, in this case, it is reasonable to consider that all MAGs provide the same security for protecting ND messages, and that either all MAGs or no MAGs will behave as a Secure ND Proxy, so configuration is expected to be easier.

A configuration option MAY exist in a Secure ND Proxy to specify the non-SEND nodes to which it is connected, so that the proxied messages sent to these nodes are not processed according to the Secure Proxy ND specification, for performance reasons.

8. Security Considerations

The mechanism described in this document introduces a new PS option allowing a Secure ND Proxy to synthesize or translate a SEND message for a proxied address, to redirect traffic for given target addresses, or to advertise prefix information by means of RA messages. An SPND node only accepts such a message if it includes a valid PS option generated by a properly authorized Secure ND Proxy (with a certificate containing a KeyPurposeId with value id-kp-sendProxiedOwner for protecting NA, NS, and RS messages, or containing a KeyPurposeId value of id-kp-sendProxiedRouter for protecting RA and Redirect messages). Such a message has protection against the threats presented in Section 9 of [RFC3971] equivalent to a message signed with an RSA Signature option.

The security of proxied ND messages not including a PS option is the same as an unsecured ND message. The security of a proxied ND message received by a non-SEND host or RFC 3971 host is the same as an unsecured ND message.

When a message including a PS option is received by an SPND node, any CGA or RSA options also included in the message are removed and the remaining message further processed. Although properly formed proxied messages MUST NOT include PS and CGA/RSA options at the same time, discarding them if they appear does not affect security. If the PS option is validated, then the information included in the message has been validly generated by a proxy, and should be honored (remember that anti-replay protection is provided by means of Nonce and Timestamp options). If the PS option is not validated, then it

is treated as an unsecured message. In any case, there is no gain for an attacker from appending false or old CGA/RSA information to a message secured by a Secure ND Proxy.

A compromised Secure ND Proxy provisioned with an authorization certificate with a KeyPurposeId value of id-kp-sendProxiedRouter is able, like a compromised router, to siphon off traffic from the host, or mount a man-in-the-middle attack, for hosts communicating to off-link hosts. A compromised Secure ND Proxy provisioned with an authorization certificate with a KeyPurposeId value of id-kp-sendProxiedOwner can siphon off traffic or mount a man-in-the-middle attack for communication between on-link hosts, even if the hosts use SEND. Note that different application scenarios may require one type of authorization, the other, or both. To minimize security risks, authorization capabilities MUST NOT exceed the ones strictly required by the application scenario to be deployed.

The messages for which a Secure ND Proxy performs its function and the link for which this function is performed MUST be configured appropriately for each proxy and scenario. This configuration is especially relevant if Secure Proxy ND is used for translating ND messages from one link to another.

Section 7 discusses the security considerations resulting from the decision to append or omit the PS option, depending on the SEND-awareness of the proxied nodes.

Protection against replay attacks from unsolicited messages such as NA, RA, and Redirects is provided by means of the Timestamp option. When Secure ND Proxy is used, each host, and each proxy acting on behalf of that host, are considered to be different peers in terms of timestamp verification. Since the information provided by the host and a proxy, including different link-layer addresses, may be different, a replay attack could affect the operation of a third node: replaying messages issued by a host that is no longer in the link can prevent the use of a proxy, and replaying messages of a proxy when the host is back in the link can prevent communication with the host. This kind of attack can be performed until the timestamp of the peer (either the host or a proxy) is no longer valid for the receiver. The window of vulnerability is in general larger for the first message received from a new peer than for subsequent messages received from the same peer (see [RFC3971]). A more detailed analysis of the possible attacks related to the Timestamp option is described in Section 6.3 of [RFC5909].

9. IANA Considerations

IANA has allocated the following a new IPv6 Neighbor Discovery Option type for the PS option, as 32. The value has been allocated from the namespace specified in the IANA "IPv6 Neighbor Discovery Option Formats" registry located at http://www.iana.org/assignments/icmpv6-parameters.

IANA has also allocated the following new 128-bit value under the "Cryptographically Generated Addresses (CGA) Message Type Name Space" registry [RFC3972]:

0x09F5 2BE5 3B62 4C76 CB96 4E7F CDC9 2804.

10. Acknowledgements

The text has benefited from feedback provided by Jari Arkko, Jean-Michel Combes, Roque Gagliano, Tony Cheneau, Marcelo Bagnulo, Alexey Melnikov, Sandra Murphy, and Sean Turner.

The work of Alberto Garcia-Martinez was supported in part by the T2C2 project (TIN2008-06739-C04-01, granted by the Spanish Science and Innovation Ministry).

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.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC4389] Thaler, D., Talwar, M., and C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389, April 2006.

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

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6494] Gagliano, R., Krishnan, S., and A. Kukec, "Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)", RFC 6494, February 2012.

[RSA] RSA Laboratories, "PKCS #1 v2.1: RSA Cryptography Standard", June 2002.

[SHA1] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-1 , April 1995.

11.2. Informative References

[RFC3756] Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RFC5909] Combes, J-M., Krishnan, S., and G. Daley, "Securing Neighbor Discovery Proxy: Problem Statement", RFC 5909, July 2010.

Authors' Addresses

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
EMail: suresh.krishnan@ericsson.com

Julien Laganier
Juniper Networks
1094 North Mathilda Avenue
Sunnyvale, CA 94089
USA

Phone: +1 408 936 0385
EMail: julien.ietf@gmail.com

Marco Bonola
Rome Tor Vergata University
Via del Politecnico, 1
Rome I-00133
Italy

Phone:
EMail: marco.bonola@gmail.com

Alberto Garcia-Martinez
U. Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
Spain

Phone: +34 91 6248782
EMail: alberto@it.uc3m.es
URI: http://www.it.uc3m.es/