IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 3971, 4861 (if approved)
Intended status: Standards Track
Expires: July 15, 2012

F. Gont
UK CPNI

January 12, 2012

# Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery

draft-gont-6man-nd-extension-headers-02

## Abstract

This document analyzes the security implications of using IPv6 Extension Headers with Neighbor Discovery (ND) messages. It updates RFC 4861 such that use of the IPv6 Fragmentation Header is forbidden in all Neighbor Discovery messages, thus allowing for simple and effective counter-measures for Neighbor Discovery attacks. Finally, it discusses the security implications of using IPv6 fragmentation with SEcure Neighbor Discovery (SEND), and provides advice such that the aforementioned security implications are mitigated.

## Status of this Memo



## Copyright Notice

Table of Contents

# 1. Introduction

The Neighbor Discovery Protocol (NDP) is specified in RFC 4861 [RFC4861] and RFC 4862 [RFC4862]. It is used by both hosts and routers. Its functions include Neighbor Discovery (ND), Router Discovery (RD), Address Autoconfiguration, Address Resolution, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and Redirection.

Many of the possible attacks against the Neighbor Discovery Protocol are discussed in detail in [RFC3756]. In order to mitigate the aforementioned possible attacks, the SEcure Neighbor Discovery (SEND) was standardized. SEND employs a number of mechanisms to certify the origin of Neighbor Discovery packets and the authority of routers, and to protect Neighbor Discovery packets from being the subject of modification or replay attacks.

However, a number of factors, such as the use of trust anchors and the unavailability of SEND implementations for many widely-deployed operating systems, make SEND hard to deploy [Gont-DEEPSEC2011]. Thus, in many general scenarios it may be necessary and/or convenient to use other mitigation techniques for NDP-based attacks. The following "lightweight" mitigations are currently available for NDP attacks:

o Layer-2 filtering of Neighbor Discovery packets (such as RA-Guard [RFC6105])

o Neighbor Discovery monitoring tools (e.g., such as NDPMon [NDPMon])

IPv6 Router Advertisement Guard (RA-Guard) is a mitigation technique for attack vectors based on ICMPv6 Router Advertisement messages. It is meant to block attack packets at a layer-2 device before the attack packets actually reach the target nodes. [RFC6104] describes the problem statement of "Rogue IPv6 Router Advertisements", and [RFC6105] specifies the "IPv6 Router Advertisement Guard" functionality.

Tools such as NDPMon [NDPMon] and ramond [ramond] aim at monitoring Neighbor Discovery traffic in the hopes of detecting possible attacks when there are discrepancies between the information advertised in Neighbor Discovery packets and the information stored on a local database.

A key challenge that these mitigation or monitoring techniques face is that introduced by IPv6 fragmentation, since it is trivial for an attacker to conceal his attack by fragmenting his packets into multiple fragments. This may limit or even eliminate the effectiveness of the aforementioned mitigation or monitoring techniques. Recent work [CPNI-IPv6] indicates that current implementations of the aforementioned "lightweight" mitigations for NDP attacks can be trivially evaded. For example, as noted in [I-D.gont-v6ops-ra-guard-implementation], current RA-Guard implementations can be trivially evaded by fragmenting the attack packets into multiple fragments, such that the layer-2 device cannot find all the necessary information to perform packet filtering in the same packet. While Neighbor Discovery monitoring tools could (in theory implement IPv6 fragment reassembly, this is usually an arms-race with the attacker (an attacker generate lots of forged fragments to "confuse" the monitoring tools), and therefore the aforementioned tools are unreliable for the detection of such attacks.

Section 2 analyzes the use of IPv6 fragmentation in traditional Neighbor discovery. Section 3 analyzes the use of IPv6 fragmentation in SEcure Neighbor Discovery (SEND). Section 4 formally updates RFC 4861 such that use of the IPv6 Fragment Header with traditional Neighbor Discovery is forbidden, and provides advice on the use of IPv6 fragmentation with SEND.

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 RFC 2119 [RFC2119].

## 2. Traditional Neighbor Discovery and IPv6 Fragmentation

The only potential use case for IPv6 fragmentation with traditional (i.e., non-SEND) IPv6 Neighbor Discovery would be that in which a Router Advertisement must include a large number of options (Prefix Information Options, Route Information Options, etc.). However, this could still be achieved without employing fragmentation, by splitting the aforementioned information into multiple Router Advertisement messages.

> Some Neighbor Discovery implementations are known to silently ignore Router Advertisement messages that employ fragmentation. Therefore, splitting the necessary information into multiple RA messages (rather than sending a large RA message that is fragmented into multiple IPv6 fragments) is probably desirable even from an interoperability point of view.

As a result of the aforementioned considerations, and since avoiding the use of IPv6 fragmentation in traditional Neighbor Discovery would greatly simplify and improve the effectiveness of monitoring and filtering ND, Section 4 specifies that hosts silently ignore traditional Neighbor Discovery messages (i.e., those specified in [RFC4861]) that employ IPv6 fragmentation.

## 3. SEcure Neighbor Discovery (SEND) and IPv6 Fragmentation

SEND packets typically carry more information than traditional Neighbor Discovery packets: for example, they include additional options such as the CGA option and the RSA signature option.

In the case of Neighbor Discovery messages specified in [RFC4861], the situation is roughly the same: if more information than would fit in a non-fragmented Neighbor Discovery packet needs to be sent, it should be split into multiple Neighbor Discovery messages (such that IPv6 fragmentation is avoided).

However, Certification Path Advertisement messages (specified in [RFC3971]) pose a different situation, since the Certificate Option they include contain much more information than any other Neighbor Discovery option. For example, Appendix C of [RFC3971] reports Certification Path Advertisement messages from 1050 to 1066 bytes on an Ethernet link layer. Since the aforementioned packet sizes are close to the minimum IPv6 MTU (1280 bytes), we note that IPv6 fragmentation must still be allowed for Certificate Path Advertisement messages.

It should be noted that relying on fragmentation opens the door to a variety of IPv6 fragmentation-based attacks. In particular, if an attacker is located on the same broadcast domain as the victim host, and Certification Path Advertisement messages employ IPv6 fragmentation, it would be trivial for the attacker to forge IPv6 fragment such that they result in "Fragment ID collisions", causing both the attack fragments and the legitimate fragments to be discarded by the victim node. This would eventually cause the Authorization Delegation Discovery to fail, thus leading the host to fall back (depending to local configuration) either to unsecured mode, or to reject the corresponding Router Advertisement messages (possibly resulting in a Denial of Service).

## 4. Specification

Nodes SHOULD NOT employ IPv6 fragmentation for sending any of the following Neighbor Discovery and SEcure Neighbor Discovery messages: Neighbor Solicitation, Neighbor Advertisement, Router Solicitation, Router Advertisement, Redirect, Certification Path Solicitation, and Certification Path Advertisement.

Nodes SHOULD silently ignore the following Neighbor Discovery and SEcure Neighbor Discovery messages if the packets carrying them include an IPv6 Fragmentation Header: Neighbor Solicitation, Neighbor Advertisement, Router Solicitation, Router Advertisement, Redirect, and Certification Path Solicitation.

Nodes SHOULD normally process Certification Path Advertisement messages that employ IPv6 fragmentation.

## 5. Security Considerations

The IPv6 Fragmentation Header can be leveraged to circumvent network monitoring tools and current implementations of mechanisms such as RA-Guard [I-D.gont-v6ops-ra-guard-implementation]. By updating the relevant specifications such that the IPv6 Fragment Header is not allowed in any Neighbor Discovery messages except "Certification Path Advertisement", protection of local nodes against Neighbor Discovery attacks, and monitoring of Neighbor Discovery traffic is greatly simplified.

[I-D.gont-v6ops-ra-guard-implementation] discusses an improvement to the RA-Guard mechanism that can mitigate Neighbor Discovery attacks that employ IPv6 Fragmentation. However, it should be noted that unless [RFC4861] is updated (as proposed in this document), Neighbor Discovery monitoring tools (such as NDPMon [NDPMon]) would remain unreliable and trivial to circumvent by a skilled attacker.

As noted in Section 3, use of SEND could potentially result in fragmented "Certification Path Advertisement" messages, thus allowing an attacker to employ IPv6 fragmentation-based attacks against such messages. Therefore, to the extent that is possible, such use of fragmentation should be avoided.

## 6. Acknowledgements

The author would like to thank (in alphabetical order) Mikael Abrahamsson, Ran Atkinson, Jean-Michel Combes, David Farmer, Bob Hinden, Philip Homburg, Ray Hunter, Arturo Servin, and Mark Smith, for providing valuable comments on earlier versions of this document.

This document resulted from the project "Security Assessment of the Internet Protocol version 6 (IPv6)" [CPNI-IPv6], carried out by Fernando Gont on behalf of the UK Centre for the Protection of National Infrastructure (CPNI). The author would like to thank the UK CPNI, for their continued support.

# 7. References

## 7.1. Normative References


[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[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.


## 7.2. Informative References


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

[RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", RFC 6104, February 2011.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, February 2011.

[NDPMon] "NDPMon - IPv6 Neighbor Discovery Protocol Monitor", <http://ndpmon.sourceforge.net/>.

[ramond] "ramond", <http://ramond.sourceforge.net/>.

[I-D.gont-v6ops-ra-guard-implementation]
Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", draft-gont-v6ops-ra-guard-implementation-00 (work in progress), January 2012.

[CPNI-IPv6]
Gont, F., "Security Assessment of the Internet Protocol version 6 (IPv6)", UK Centre for the Protection of National Infrastructure, (available on request).

[Gont-DEEPSEC2011]
Gont, "Results of a Security Assessment of the Internet

Protocol version 6 (IPv6)",  DEEPSEC 2011 Conference,
Vienna, Austria, November 2011, <http://
www.si6networks.com/presentations/deepsec2011/
fgont-deepsec2011-ipv6-security.pdf>.

# Appendix A. Changes from previous versions of the draft (to be removed by the RFC Editor before publication of this document as a RFC

## A.1. Changes from draft-gont-6man-nd-extension-headers-01

- The I-D now forbids only the Fragment Header (rather than all Extension Headers) with most ND packets.

- A discussion of the use of IPv6 fragmentation with ND and SEND was added.

- Text was added noting that if SEND traffic is fragmented, this would open the door to fragmentation-based attacks, which would lead to trivial DoS attacks.

- Minor editorial changes

## A.2. Changes from draft-gont-6man-nd-extension-headers-00

- The Security Considerations section now notes that unless IPv6 extension headers are not allowed with Neighbor Discovery messages, monitoring ND traffic and/or mitigating ND vulnerabilities might result in increased complexity and/or reduced performance.

- Minor editorial changes

## Author's Address

Fernando Gont
Centre for the Protection of National Infrastructure

Email: fernando@gont.com.ar
URI:   http://www.cpni.gov.uk