IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 4861 (if approved)
Intended status: Standards Track
Expires: December 10, 2011

F. Gont
UK CPNI

June 8, 2011

Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery
draft-gont-6man-nd-extension-headers-01

Abstract

IPv6 Extension Headers with Neighbor Discovery messages can be leveraged to circumvent simple local network protections, such as "Router Advertisement Guard". Since there is no legitimate use for IPv6 Extension Headers in Neighbor Discovery messages, and such use greatly complicates network monitoring and simple security mitigations such as RA-Guard, this document proposes that hosts silently ignore Neighbor Discovery messages that use IPv6 Extension Headers.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

IPv6 Router Advertisement Guard (RA-Guard) is a mitigation technique for attack vectors based on ICMPv6 Router Advertisement messages. [RFC6104] describes the problem statement of "Rogue IPv6 Router Advertisements", and [RFC6105] specifies the "IPv6 Router Advertisement Guard" functionality.

[I-D.gont-v6ops-ra-guard-evasion] describes how IPv6 Extension Headers can be leveraged to circumvent the RA-Guard protection. Additionally, the use of Extension Headers (and of the Fragmentation Header in particularly) greatly increases the difficulty to monitor Neighbor Discovery traffic (e.g., with tools such as NDPMon [NDPMon]).

Since there is no current legitimate use for IPv6 Extension Headers in IPv6 Neighbor Discovery packets, and avoiding their use in such packets would greatly simplify the monitoring and mitigation of Neighbor Discovery attacks, this document proposes that hosts silently ignore Neighbor Discovery messages that employ IPv6 Extension Headers.

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. Specification

Hosts SHOULD silently ignore Neighbor Discovery messages (Neighbor Solicitation, Neighbor Advertisement, Router Solcicitation, and Router Advertisement messages) that employ IPv6 Extension Headers.

3. Security Considerations

IPv6 Extension Headers can be leveraged to circumvent network monitoring and mechanisms such as RA-Guard [I-D.gont-v6ops-ra-guard-evasion]. By updating the relevant specifications such that IPv6 Extension Headers are not allowed in Neighbor Discovery messages, protection of local network against Neighbor Discovery attacks, and monitoring of Neighbor Discovery traffic is greatly simplified.

[I-D.gont-v6ops-ra-guard-evasion] discusses an improvement to the RA-Guard mechanism that can mitigate Neighbor Discovery attacks that employ IPv6 Extension Headers. However, it should be noted that unless [RFC4861] is updated (as proposed in this document) such that use of IPv6 extension headers is not allowed with Neighbor Discovery messages, monitoring of Neighbor Discovery traffic and mitigation of Neighbor Discovery vulnerabilities will probably imply increased complexity and/or reduced performance in the corresponding devices (RA-Guard box, Network Intrusion Detection Systems, etc.).

4. Acknowledgements

The author would like to thank Arturo Servin 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.

5. References

5.1. Normative References

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

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

5.2. Informative References

[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/>.

[I-D.gont-v6ops-ra-guard-evasion] Gont, F. and U. CPNI, "IPv6 Router Advertisement Guard (RA-Guard) Evasion", draft-gont-v6ops-ra-guard-evasion-00 (work in progress), May 2011.

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

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-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.gont.com.ar