Internet Engineering Task Force (IETF)
Request for Comments: 6980
Updates: 3971, 4861
Category: Standards Track
ISSN: 2070-1721

F. Gont
SI6 Networks / UTN-FRH

August 2013

Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery

Abstract

This document analyzes the security implications of employing IPv6 fragmentation 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 countermeasures for Neighbor Discovery attacks. Finally, it discusses the security implications of using IPv6 fragmentation with SEcure Neighbor Discovery (SEND) and formally updates RFC 3971 to provide advice regarding how the aforementioned security implications can be mitigated.

Status of This Memo

Table of Contents

1. Introduction

The Neighbor Discovery Protocol (NDP) is specified in RFC 4861 [RFC4861]. 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, 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 high administrative overhead of deploying trust anchors and the unavailability of SEND implementations for many widely deployed operating systems, make SEND hard to deploy [Gont-DPSC]. Thus, in many general scenarios, it may be necessary and/or convenient to use other mitigation techniques for NDP-based attacks. The following mitigations are currently available for NDP attacks:

- Static Access Control Lists (ACLs) in switches

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

- Neighbor Discovery monitoring tools (e.g., NDPMon [NDPMon] and ramond [ramond])

- Intrusion Prevention Systems (IPS)

IPv6 Router Advertisement Guard (RA-Guard) is a mitigation technique for attack vectors based on ICMPv6 Router Advertisement (RA) 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 to monitor 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.

Some Intrusion Prevention Systems (IPS) can mitigate Neighbor Discovery attacks. We recommend that Intrusion Prevention Systems implement mitigations for NDP attacks.

IPv6 fragmentation introduces a key challenge for these mitigation or monitoring techniques, 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 mitigations for NDP attacks can be trivially evaded. For example, as noted in [RA-GUARD], 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 can 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 provides the rationale for forbidding the use of IPv6 fragmentation with Neighbor Discovery. Section 5 formally updates RFC 4861 such that the use of the IPv6 Fragment Header with traditional Neighbor Discovery is forbidden, and also formally updates RFC 3971 by providing advice on the use of IPv6 fragmentation with SEND. Section 6 provides operational advice about interoperability problems arising from the use of IPv6 fragmentation with Neighbor Discovery.

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.

Thus, avoiding the use of IPv6 fragmentation in traditional Neighbor Discovery would greatly simplify and improve the effectiveness of monitoring and filtering Neighbor Discovery traffic and would also prevent interoperability problems with those implementations that do not support fragmentation in Neighbor Discovery messages.

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 Cryptographically Generated Address (CGA) option and the RSA signature option.

When SEND nodes employ any of the 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 (CPA) messages (specified in [RFC3971]) pose a different situation, since the Certificate Option they include typically contains 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 size of CPA messages could potentially exceed the MTU of the local link, Section 5 recommends that fragmented CPA messages be processed normally, but discourages the use of keys that would result in fragmented CPA messages.

It should be noted that relying on fragmentation opens the door to a variety of IPv6 fragmentation-based attacks against SEND. 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 fragments 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 Authorization Delegation Discovery (Section 6 of [RFC3971]) to fail, thus leading the host to (depending on local configuration) either fall back to unsecured mode or reject the corresponding Router Advertisement messages (possibly resulting in a denial of service).

4. Rationale for Forbidding IPv6 Fragmentation in Neighbor Discovery

A number of considerations should be made regarding the use of IPv6 fragmentation with Neighbor Discovery:

- A significant number of existing implementations already silently drop fragmented ND messages, so the use of IPv6 fragmentation may hamper interoperability among IPv6 implementations.

- Although it is possible to build an ND message that needs to be fragmented, such packets are unlikely to exist in the real world because of the large number of options that would be required for the resulting packet to exceed the minimum IPv6 MTU of 1280 octets.

- If an ND message was so large as to need fragmentation, there is an option to distribute the same information amongst more than one message, each of which is small enough to not need fragmentation.

Thus, forbidding the use of IPv6 fragmentation with Neighbor Discovery normalizes existing behavior and sets the expectations of all implementations to the existing lowest common denominator.

5. Specification

Nodes MUST 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

Nodes SHOULD NOT employ IPv6 fragmentation for sending the following messages (see Section 6.4.2 of [RFC3971]):

- Certification Path Advertisement

Nodes MUST 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
- Certification Path Solicitation

Nodes SHOULD normally process the following messages when the packets carrying them include an IPv6 Fragmentation Header:

- Certification Path Advertisement

SEND nodes SHOULD NOT employ keys that would result in fragmented CPA messages.

6. Operational Advice

An operator detecting that Neighbor Discovery traffic is being silently dropped should find whether the corresponding Neighbor Discovery messages are employing IPv6 fragmentation. If they are, it is likely that the devices receiving such packets are silently dropping them merely because they employ IPv6 fragmentation. In such a case, an operator should check whether the sending device has an option to prevent fragmentation of ND messages, and/or see whether it is possible to reduce the options carried on such messages. We note that solving this (unlikely) problem might require a software upgrade to a version that does not employ IPv6 fragmentation with Neighbor Discovery.

7. Security Considerations

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

As noted in Section 3, the 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.

8. Acknowledgements

The author would like to thank (in alphabetical order) Mikael Abrahamsson, Ran Atkinson, Ron Bonica, Jean-Michel Combes, David Farmer, Adrian Farrel, Stephen Farrell, Roque Gagliano, Brian Haberman, Bob Hinden, Philip Homburg, Ray Hunter, Arturo Servin, Mark Smith, and Martin Stiemerling for providing valuable comments on earlier versions of this document.

The author would also like to thank Roque Gagliano for contributing the information regarding message sizes in Appendix A, and Arturo Servin for presenting this document at IETF 81.

Finally, the author would like to thank his brother, friend, and colleague, Guillermo Gont, for his love and support.

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).

9. References

9.1. 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.

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

9.2. Informative References

[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-DPSC] Gont, F., "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>.

[NDPMon] SourceForge, "NDPMon - IPv6 Neighbor Discovery Protocol Monitor", July 2012, <http://ndpmon.sourceforge.net/>.

[RA-GUARD] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", Work in Progress, November 2012.

[ramond] SourceForge, "ramond", January 2009, <http://ramond.sourceforge.net/>.

[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.

Appendix A. Message Size When Carrying Certificates

This section aims at estimating the size of normal Certification Path Advertisement messages.

Considering a Certification Path Advertisement (CPA) such as that of Appendix C of [RFC3971] (certification path length of 4, between 1 and 4 address prefix extensions, and a key length of 1024 bits), the certificate lengths range between 864 and 888 bytes (and the corresponding Ethernet packets from 1050 to 1066 bytes) [RFC3971].

Updating the aforementioned packet size to account for the larger (2048 bits) keys required by [RFC6494] results in packet sizes ranging from 1127 to 1238 bytes, which are smaller than the minimum IPv6 MTU (1280 bytes) and much smaller than the ubiquitous Ethernet MTU (1500 bytes).

However, we note that packet sizes may vary depending on a number of factors, including:

- o the number of prefixes included in the certificate
- o the length of Fully Qualified Domain Names (FQDNs) in Trust Anchor (TA) options [RFC3971] (if present)

If larger key sizes (e.g., 4096 bits) are required in the future, a larger MTU size might be required to convey such information in Neighbor Discovery packets without the need to employ fragmentation.

Author's Address

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
EMail: fgont@si6networks.com
URI: http://www.si6networks.com