

V60PS Work Group
Internet Draft
Intended status: Standard Stack
Expires: August 28, 2010

S. Jiang
X. Chen
X. Song
Huawei Technologies Co., Ltd
March 2, 2010

Neighbor Cache Protection in Neighbor Discover Protocol
draft-jiang-v6ops-nc-protection-01.txt

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/lid-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 August 28, 2010.

Copyright Notice

Copyright (c) 2010 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 BSD License.

Internet-Draft [draft-jiang-v6ops-nc-protection-01.txt](#)

March 2010

Abstract

In Neighbor Discover Protocol, routers and hosts record the neighbor information in the local Neighbor Cache database. It is vulnerable by malicious attacks. This document analyzes these security threats and proposes a solution, mainly using reverse detection mechanism, to prevent the potential damage.

Table of Contents

1.	Introduction.....	3
2.	Terminology.....	3
3.	Motivations and Issues.....	3
4.	Solution: Reverse Detection.....	4
5.	Additional Discussion.....	5
5.1.	Exceptional LLAs.....	5
5.2.	Looped reverse detection.....	6
5.3.	Rate limit for incoming NS.....	6
5.4.	CPU & memory protection.....	6
6.	Security Considerations.....	6
7.	IANA Considerations.....	6
8.	Change Log [RFC Editor please remove].....	7
9.	References.....	7
9.1.	Normative References.....	7
9.2.	Informative References.....	7
	Author's Addresses.....	8

[1.](#) Introduction

In Neighbor Discover protocol (ND, [[RFC4861](#)]), routers and hosts record the neighbor information in the local Neighbor Cache (NC) database. It is vulnerable by DOS attacks. In the current definition, it is difficult to detect whether the neighbor information are from a real neighbor or a faked attacker. This document analyzes these security threats. Although SEcure Neighbor Discovery Protocol (SEND) is defined as upgrade/replaced version of ND, it is very complicated and does not widely deployed yet.

This document proposes a Neighbor Cache protection solution, mainly using reverse detection mechanism, to prevent the potential damage. This solution is based on the procedures that already defined in the current ND definition, so it is fully compatible with ND. This design principle allows that most of network devices remain on their current ND implementation, only the devices that need advanced NC protection apply the proposed mechanism.

[2.](#) Terminology

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](#) [[RFC2119](#)].

[3.](#) Neighbor Cache Threats

In the IPv6 edge network, hosts and routers use Neighbor Discovery protocol to resolve the neighbors known to reside on attached links. The neighbors' information, such as the paired mapping of link-layer addresses and IPv6 addresses, is recorded in a local Neighbor Cache database.

However, the NC is vulnerable by malicious attacks. A Denial of Service (DoS) attack against the NC of an IPv6 node (host or router) can fill up with faked entries and exhaust the cache's resources.

This interrupts the normal functions of the targeted IPv6 node. If the attack is successful in overwhelming a forwarding router, the edge network may be disconnected from the global Internet. By sending a faked Neighbor Solicitation message, an attacker can make the target node allocate a Neighbor Cache entry for a period of time. If the attacker repeats the procedure using faked IPv6 addresses, the NC will grow. Eventually the NC exhausts all memory allocated for it. The same risks exist on proxies and normal hosts that implement Neighbor Discovery protocol.

For example, if the attackers send minimally sized Neighbor Solicitation (NS) packets, which is 90 Bytes (14-Byte Ethernet header, 40B IPv6 header, 32B NS message, 4B trailer), to target router on a 100 Mbps Ethernet link, it can, in theory, build up and sustain perhaps 145k bogus entries in the target's NC. Given that each entry contains at least one Ipv6 address, one MAC address, a state and a few flags, approximately 50 Bytes, this puts memory usage up in the range of 8 MB in this example. This illustrates the scale of the problems an attacker can cause on one interface. An attack on many interfaces that is paired with distributed attackers will be manifold worse.

DoS is the most considerable threat among with many others, analyzed in Threats Analysis, [Section 11.1](#), in [\[RFC4861\]](#). SeND [\[RFC3971\]](#) provides a feasible solution to these problems, based on certification anchors on every network devices. It does require all nodes on a local network to support SeND. The provision of certificate anchors on every network devices is a tough deployment challenges while there are secure issues for itself.

[4.](#) Security Requirements

Accordingly, it would be desirable to provide a defending mechanism against DoS attacks targeting Neighbor Caches. This mechanism SHOULD meet at least anti Dos, anti replay and anti spoofing (L3 spoofing) requirements.

The focus for this effort, and the scope for this document explicitly excludes, at this point in time, privacy (or encryption), authentication, message integrity and non-repudiation.

[5.](#) Solution: Reverse Detection

In order to protect the NC against malicious attacks, a Reverse Detection (RD) mechanism is introduced. This solution is based on the messages and the procedures that already defined in the current ND definition, so it is fully compatible with ND. This design principle allows that most of network devices remain on their current ND implementation, only the devices that need advanced NC protection apply the proposed mechanism. The following figure illustrates the NC protection mechanism on a router. (The protected network devices may be a host or a proxy [RFC4389] that implements ND protocol, besides a router.)

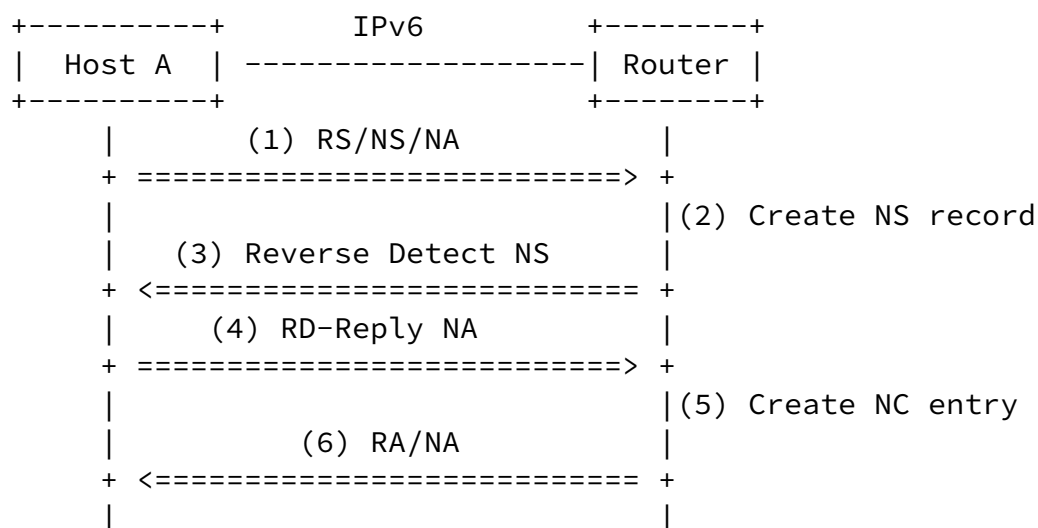


Figure: the example of reverse detection for NC protection

In the current ND definition, when a router received a RS (Router Solicitation) / NS / NA (Neighbor Advertisement) message (action (1) in the figure), it creates a new NC entry locally (action (5) in the figure) and reply a RA (Router Advertisement) / NA to the node that initiates this RS/NS/NA message action (6) in the figure).

According to the analysis in the [Section 3](#), the RS/NS/NA message is not verified at all. Attacks may be carried in these messages. A RD procedure is added after the action (1). By receive the first RS/NS/NA message, the router puts this message into a high speed NS record table (action (2) in the figure). It then sends a RD NS

message to the initiated host (action (3) in the figure). The initiated host responds a NS-replied NA message (action (4) in the figure)

When the router received the RD-replied NA message, it decides whether the pair of the source IPv6 address and the source MAC address matches any entry in the NS records table. If so, fetch the matched NS record and continue the normal CPU-based slow path NS procedure (action (5) and (6) in the figure).

6. Additional Discussion

6.1. Exceptional LLAs

Before the reverse detection, the router MAY check whether the correspondent MAC address is in the local exceptional LLA table, which stores a few high priority LLAs. If the NS message is from one of such LLAs, the router SHOULD bypass the RD process.

This saves message interaction delay for these high priority or trustable hosts.

6.2. Looped reverse detection

If the initiated host is also NC protected, the reverse detection described, in the [Section 4](#), may be looped between the two devices. In order to avoid the reverse detection loop, the Reverse Detection message should be distinguished from other NS message and should not initiate another RD procedure.

6.3. Rate limit for incoming NS

As a complementary method to Reverse Detection, router NC can be protected by rate limiting NS traffic up to an acceptable threshold. Configurable access rate allows for NS traffic to be matched based on router interface or same LLA.

6.4. CPU & memory protection

The router may actively drop the NS, even it is valid, according to the CPU or memory usage status. It prevents the target device from

functioning properly due to CPU deadlock or memory exhaustion.

7. Security Considerations

The proposed NC protection mechanism may increase the new attack mechanism based on the RD procedure: an attacker may send numerous RD-NS messages to try to block a target. However, the reply procedure of RD-NS consumes little CPU and memory. The attacker have to use more resources to feasible such attack. The security risk of such attack is very low.

The proposed NC protection mechanism cannot fully prevent the attacks from MAC-spoofing attackers since their NS messages are no different from the normal valid NS messages and they are able to respond to RD-NS messages. However, the RD NC protection mechanism greatly reduces the security risk from such attackers. It forces that the attackers wait RD procedures completed before they can change their MAC addresses for the next round attack.

8. IANA Considerations

This draft does not request any IANA action.

9. Change Log [RFC Editor please remove]

[draft-jiang-v6ops-nc-protection-00](#), original version, 2009-09-19

[draft-jiang-v6ops-nc-protection-01](#), update version, 2010-03-02

10. References

10.1. Normative References

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

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

[RFC4861] T. Narten, E. Nordmark, W. Simpson and H. Soliman,

"Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#),
September 2007.

[10.2](#). Informative References

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

Jiang, et al.

Expires August 28, 2010

[Page 7]

Internet-Draft [draft-jiang-v6ops-nc-protection-01.txt](#)

March 2010

Author's Addresses

Sheng Jiang
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxu Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82836081
Email: shengjiang@huawei.com

Xu Chen
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxu Rd.,

Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82836074
Email: chenxu0128@huawei.com

Xuan Song
Huawei Technologies Co., Ltd
Huawei Building, No.3 Xinxu Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82832817
Email: songxuan@huawei.com