

IPv6 Maintenance	F. Baker	
Internet-Draft	Cisco Systems	
Intended status: Informational	July 28, 2009	
Expires: January 29, 2010		

[TOC](#)

Session Hijack in Neighbor Discovery **draft-baker-ipv6-nd-session-hijack-00**

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 January 29, 2010.

Copyright Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (<http://trustee.ietf.org/license-info>). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This memo is to point out a security issue in IPv6 Neighbor Discovery.

Table of Contents

- [1.](#) Introduction
- [2.](#) Session Hijack via Neighbor Discovery
- [3.](#) Possible mitigations

- [4.](#) IANA Considerations
- [5.](#) Security Considerations
- [6.](#) Acknowledgements
- [7.](#) References
 - [7.1.](#) Normative References
 - [7.2.](#) Informative References
- [8.](#) Author's Address

1. Introduction

[TOC](#)

This memo, which augments [\[RFC3756\]](#) (Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats," May 2004.), is to point out a security issue in IPv6 (Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," December 1998.) [RFC2460], Neighbor Discovery (Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," September 2007.) [RFC4861] and Secure Neighbor Discovery (Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)," March 2005.) [RFC3971].

2. Session Hijack via Neighbor Discovery

[TOC](#)

The attack is as follows. Imagine a LAN (wired or wireless, switched or direct) like [Figure 1 \(Sample local session\)](#) or [Figure 2 \(Sample remote session\)](#).

```

/---+-----+-----+---/
    |         |         |
+---+---+ +---+---+ +---+---+
|Host 1| |Host 2| |Host 3|
+-----+ +-----+ +-----+
```

Figure 1: Sample local session

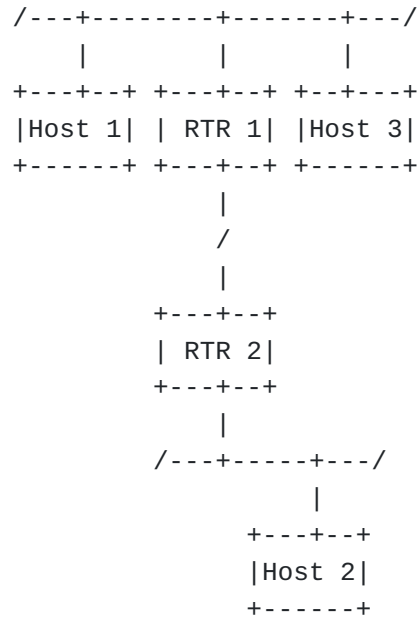


Figure 2: Sample remote session

Host 1 properly allocates an address by whatever means including manual configuration, DHCPv6, SeND, or ND, and uses the address to open a session with Host 2. The fact that it has allocated the address is observed by Host 3, perhaps by receipt of a Neighbor Solicitation during Duplicate Address Detection.

Host 1 now experiences a link-down event, losing the use of the address. This might be because the switch rebooted, Host 1's connectivity to the LAN was temporarily lost, or because Host 1 itself failed.

Host 3 now issues a Neighbor Solicitation for Host 1's address, and because Host 1 has lost its memory of the address or is unavailable at the time the request goes out. It has therefore correctly allocated the address to itself.

In this case, it would appear that the session between Host 1 and Host 2 is transferred, so that it is now between Host 2 and Host 3.

3. Possible mitigations

[TOC](#)

First one should note that in a cloud computing environment this may be an intended behavior. If it is unintended, it constitutes an attack. There are a number of possible mitigations:

- *Obviously, if the hosts have any form of session security including IPsec AH, IPsec ESP, TLS, etc, the applications will be

prevented from communicating. Host 3 will still, however, be aware that the sessions existed.

*Neighbor Discovery could be augmented to prevent movement of the IPv6 address from one MAC Address to another without an application-obvious hiccup.

*If a SAVI switch is in use, the SAVI behavior could similarly be extended to prevent the movement of the address from Host 1 to Host 3 without an application-obvious hiccup.

4. IANA Considerations

[TOC](#)

This memo asks the IANA for no new parameters.

Note to RFC Editor: This section will have served its purpose if it correctly tells IANA that no new assignments or registries are required, or if those assignments or registries are created during the RFC publication process. From the author's perspective, it may therefore be removed upon publication as an RFC at the RFC Editor's discretion.

5. Security Considerations

[TOC](#)

This note augments [\[RFC3756\] \(Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery \(ND\) Trust Models and Threats," May 2004.\)](#), and constitutes a security consideration.

6. Acknowledgements

[TOC](#)

The observation came out of a discussion regarding threats in a SAVI environment, among the author, Jun Bi, Guang Yao, and Eric Levy-Abegnoli.

7. References

[TOC](#)

7.1. Normative References

[TOC](#)

[RFC2460]	Deering, S. and R. Hinden , " Internet Protocol, Version 6 (IPv6) Specification ," RFC 2460, December 1998 (TXT , HTML , XML).
-----------	--

7.2. Informative References

[TOC](#)

[RFC3756]	Nikander, P., Kempf, J., and E. Nordmark, " IPv6 Neighbor Discovery (ND) Trust Models and Threats ," RFC 3756, May 2004 (TXT).
[RFC3971]	Arkko, J., Kempf, J., Zill, B., and P. Nikander, " SEcure Neighbor Discovery (SEND) ," RFC 3971, March 2005 (TXT).
[RFC4861]	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, " Neighbor Discovery for IP version 6 (IPv6) ," RFC 4861, September 2007 (TXT).

Author's Address

[TOC](#)

	Fred Baker
	Cisco Systems
	Santa Barbara, California 93117
	USA
Email:	fred@cisco.com