Operations Security Working Group
(opsec)
Internet-Draft
Intended status: BCP
Expires: December 7, 2012

F. Gont
SI6 Networks / UTN-FRH

June 5, 2012

Neighbor Discovery Shield (ND-Shield): Protecting against Neighbor Discovery Attacks
draft-gont-opsec-ipv6-nd-shield-00

Abstract

This document specifies a mechanism that can be implemented in layer-2 devices to mitigate attack vectors based on Neighbor Discovery messages. It is meant to complement other mechanisms implemented in layer-2 devices such as Router Advertisement Guard (RA-Guard) and DHCPv6-Shield, with the goal of achieving a comprehensive IPv6 First Hop Security solution. This document is motivated by the desire to achieve feature parity with IPv4 with respect to First Hop Security mechanisms.

Table of Contents

1. DISCLAIMER

This documents is heavily based on [I-D.ietf-v6ops-ra-guard-implementation] which, at the time of this writing, is going through IETF LC. Future revisions of this document will addresses any issues raised for [I-D.ietf-v6ops-ra-guard-implementation] which apply to this document.

Some meta-issues that require input are:

- The current version of this document specifies the filtering of different Neighbor Discovery messages in different sections. While this approach results in better-scoped rules, it might not lead to a straightforward implementation.
  - Should we coalesce all filtering rules in a single section? (and if anything, clarify how each message is processed in an appendix).
  - Even if we don't proceed that way, should similar text (e.g. all the discussion right after the filtering rules, in each of the sections) be coalesced in a single 'general' section? -- This might help reduce lots of duplicated text, make the document shorter, etc.

2. Introduction

First hop security techniques are well-known and widely implemented and deployed in the IPv4 world. For example, a number of implementations exist that allow a layer-2 device to block forged ARP reply packets that would otherwise poison the ARP cache of the victim [ARP-VULN]. Additionally, a number of implementations allow a layer-2 device to limit the number of link-layer Source Addresses that can be concurrently "in use" at any point in time on a specific layer-2 port, or the number of IP addresses that can be concurrently in use on a specific layer-2 port. Therefore, it is desirable that the same mitigation techniques be available in the IPv6 world, such that those networks currently employing these techniques can enforce the same /policies for the IPv6 protocols.

This document specifies "Neighbor Discovery Shield (ND-Shield)", a mechanism that can be employed by layer-2 devices to mitigate attacks based on the Neighbor Discovery Protocol. Specifically, this mechanism allows the filtering of malicious Router Solicitation, Neighbor Solicitation, Neighbor Advertisement, and ICMPv6 Redirect messages at a layer-2 device.

> Filtering of Router Advertisement messages is part of Router Advertisement Guard (RA-Guard) [RFC6104] [RFC6105] [I-D.ietf-v6ops-ra-guard-implementation], and hence is not specified in this document. In the same way, filtering of DHCPv6 packets is part of DHCPv6-Shield [I-D.gont-opsec-dhcpv6-shield], and hence is not specified in this document.

The basic concept behind ND-Shield is that a layer-2 device can filter Neighbor Solicitation, Neighbor Advertisement, and Redirect messages, according to a number of different criteria, such as whether the Target Address or the Source Link-Layer address fields of the corresponding message are considered legitimate, or whether the corresponding ICMPv6 type/code message is to be allowed on a specific layer-2 port.

Section 3 discusses the type of attacks that ND-Shield is expected to mitigate. Section 4 discusses the importance of deploying ND-Shield in those networks currently employing RA-Guard and/or DHCPv6-Shield. Section 5 specifies the Neighbor Discovery Guard (ND-Guard) mechanism; that is, the filtering rules to be enforced on the local layer-2 device such that attacks based on Router Solicitation, Neighbor Solicitation, Neighbor Advertisement, and Redirect messages are mitigated.

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].

3. Mitigating attacks based on the Neighbor Discovery Protocol

This section provides a brief summary of the types of attacks that ND-Shield is expected to mitigate.

3.1. Neighbor Discovery Cache Poisoning attacks

An attacker could cause a victim node to include an illegitimate entry in the Neighbor Cache, by sending a Neighbor Solicitation or Router Solicitation with a forged Source Link-Layer Address option or a Neighbor Advertisement or REdirect message with a forged Target Link-Layer address option. This attack could be exploited for Denial of Service (DoS) or Man In The Middle (MITM) purposes.

3.2. Routing Denial of Service (DoS) attacks

An attacker could cause a victim node to disable its first-hop router by sending a forged Neighor Advertisement with the 'R' flag clear.

3.3. Redirect Attacks

An attacker could cause a victim node to send its packets to a different (and possibly malicious) "first hop router" by sending forged Redirect messages. This attack could be exploited for Denial of Service (DoS) or Man In The Middle (MITM) purposes.

4. Importance of Deploying ND-Shield along with RA-Guard and DHCPv6-Shield

RA-Guard [RFC6105] [I-D.ietf-v6ops-ra-guard-implementation] can mitigate attack vectors based on ICMPv6 Router Advertisement messages by blocking Router Advertisement messages received on "unauthorized" layer-2 ports. Thus, RA-Guard can mitigate attacks where a malicious node tries to convey illegitimate network configuration information to the victim nodes. In a similar way, DHCPv6-Shield [I-D.gont-opsec-dhcpv6-shield] can mitigate attack vectors based on forged DHCPv6 messages, where the attacker tries to convey illegitimate network configuration information to the victim nodes.

However, even if Router Advertisement and DHCPv6 messages are policed, an attacker could still e.g. divert traffic meant to the legitimate router to a node he controls by sending forged Neighbor Advertisement messages that illegitimately map the first-hop router's IPv6 address to a the link-layer address of an attacker-controlled node or by sending forged Redirect messages that cause a per-host specific route to be created at the victim node.

Therefore, deployment of ND-Shield in scenarios where RA-Guard and/or DHCPv6-Shield are already deployed is highly recommended.

5. Neighbor Discovery Shield (ND-Shield) Specification

The following subsections specify the filtering rules MUST be implemented as part of an "ND-Shield" implementation.

5.1. Filtering Router Solicitation Messages

1. If the Hop Limit is not 255, pass the packet.

   Section 6.1.1 of [RFC4861] requires nodes to discard Router Solicitation messages if their Hop Limit is not 255.

2. Try to identify whether the packet is an ICMPv6 Router Solicitation message, by parsing the IPv6 header chain. When doing so, enforce a limit on the maximum number of Extension Headers that is allowed for each packet, and if such limit is hit before the upper-layer protocol is identified, drop the packet.

   [RFC6564] specifies a uniform format for IPv6 Extension Header, thus meaning that an IPv6 node should be able to parse an IPv6 header chain even if it contains Extension Headers that are not currently supported by that node.

3. If ND-Shield is unable to identify whether the packet is an ICMPv6 Router Solicitation message or not (i.e., the packet is a first-fragment, and the necessary information is missing), drop the packet.

   Note: This rule should only be applied to non-fragmented IPv6 datagrams and IPv6 fragments with a Fragment Offset of 0 (non-first fragments can be safely passed, since they will never reassemble into a complete datagram if they are part of a Router Solicitation message of which the first fragment was dropped).

4. If the packet is identified to be an ICMPv6 Router Solicitation message, then proceed as follows:

   1. If the Source Address is the loopback address (::1) or a multicast address, drop the packet.

      Such addresses are invalid for Router Solicitation messages, and dropping these illegitimate packets here simplifies the nest filtering rules.

   2. If the Source Address is a unicast address which is not known to be in use at any of the layer-2 ports, record the Source Address as being in use on the received port, and pass the

packet as usual.

3. If the Source Address is a unicast address which is known to be in use on a layer-2 port other than the one on which the packet was received, drop the received packet.

5. In all other cases, pass the packet as usual.

Note: For the purpose of enforcing the ND-Shield filtering policy, an ESP header [RFC4303] should be considered to be an "upper-layer protocol" (that is, it should be considered the last header in the IPv6 header chain). This means that packets employing ESP would be passed by the ND-Shield device to the intended destination. If the destination host does not have a security association with the sender of the aforementioned IPv6 packet, the packet would be dropped. Otherwise, if the packet is considered valid by the IPsec implementation at the receiving host and encapsulates a Router Solicitation message, it is up to the receiving host what to do with such packet.

If a packet is dropped due to this filtering policy, then the packet drop event SHOULD be logged. The logging mechanism SHOULD include a drop counter dedicated to ND-Shield packet drops.

In order to protect current end-node IPv6 implementations, Rule #4 has been defined as a default rule to drop packets that cannot be positively identified as not being Router Solicitation (RS) messages (possibly because the packet contains fragments that do not contain the entire IPv6 header chain). This means that, at least in theory, ND-Shield could result in false-positive blocking of some legitimate non-RS packets that could not be positively identified as being non-RS. In order to reduce the likelihood of false positives, Rule #1 requires that packets that would not pass the required validation checks for RS messages (Section 6.1.1 of [RFC4861]) be passed without further inspection. In any case, as noted in [I-D.gont-6man-oversized-header-chain], IPv6 packets that fail to include the entire IPv6 header chain are anyway unlikely to survive in real networks. Whilst currently legitimate from a specifications standpoint, they are virtually impossible to police with state-less filters and firewalls, and are hence likely to be blocked by such filters and firewalls.

This filtering policy assumes that host implementations require the Hop Limit of Neighbor Discovery messages to be 255, and discard those packets otherwise.

The aforementioned filtering rules implicitly handle the case of fragmented packets: if the ND-Shield device fails to identify the

upper-layer protocol as a result of the use of fragmentation, the corresponding packets would be dropped.

Finally, we note that IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [RFC5722]) might still be subject of RS-based attacks. However, a recent assessment of IPv6 implementations [SI6-FRAG] with respect to their fragment reassembly policy seems to indicate that most current implementations comply with [RFC5722].

5.2. Filtering Neighbor Solicitation Messages

1. If the Hop Limit is not 255, pass the packet.

   Section 7.1.1 of [RFC4861] requires nodes to discard Neighbor Solicitation messages if their Hop Limit is not 255.

2. Try to identify whether the packet is an ICMPv6 Neighbor Solicitation message, by parsing the IPv6 header chain. When doing so, enforce a limit on the maximum number of Extension Headers that is allowed for each packet, and if such limit is hit before the upper-layer protocol is identified, drop the packet.

   [RFC6564] specifies a uniform format for IPv6 Extension Header, thus meaning that an IPv6 node should be able to parse an IPv6 header chain even if it contains Extension Headers that are not currently supported by that node.

3. If ND-Shield is unable to identify whether the packet is an ICMPv6 Neighbor Solicitation message or not (i.e., the packet is a first-fragment, and the necessary information is missing), drop the packet.

   Note: This rule should only be applied to non-fragmented IPv6 datagrams and IPv6 fragments with a Fragment Offset of 0 (non-first fragments can be safely passed, since they will never reassemble into a complete datagram if they are part of a Neighbor Solicitation message of which the first fragment was dropped).

4. If the packet is identified to be an ICMPv6 Neighbor Solicitation message, then proceed as follows:

   1. If the Source Address is the unspecified address, and the Destination Address is not a solicited-node multicast address or the packet contains source link-layer address option, drop the packet.

2. If the Source Address is a unicast address which is not known to be in use at any of the layer-2 ports, record the Source Address as being in use on the received port, and pass the packet as usual.

3. If the Source Address is a unicast address which is known to be in use on a layer-2 port other than the one on which the packet was received, drop the received packet.

5. In all other cases, pass the packet as usual.

Note: For the purpose of enforcing the ND-Shield filtering policy, an ESP header [RFC4303] should be considered to be an "upper-layer protocol" (that is, it should be considered the last header in the IPv6 header chain). This means that packets employing ESP would be passed by the ND-Shield device to the intended destination. If the destination host does not have a security association with the sender of the aforementioned IPv6 packet, the packet would be dropped. Otherwise, if the packet is considered valid by the IPsec implementation at the receiving host and encapsulates a Router Advertisement message, it is up to the receiving host what to do with such packet.

If a packet is dropped due to this filtering policy, then the packet drop event SHOULD be logged. The logging mechanism SHOULD include a drop counter dedicated to ND-Shield packet drops.

In order to protect current end-node IPv6 implementations, Rule #4 has been defined as a default rule to drop packets that cannot be positively identified as not being Neighbor Solicitation (NS) messages (possibly because the packet contains fragments that do not contain the entire IPv6 header chain). This means that, at least in theory, ND-Shield could result in false-positive blocking of some legitimate non-NS packets that could not be positively identified as being non-NS. In order to reduce the likelihood of false positives, Rule #1 requires that packets that would not pass the required validation checks for NS messages (Section 7.1.1 of [RFC4861]) be passed without further inspection. In any case, as noted in [I-D.gont-6man-oversized-header-chain], IPv6 packets that fail to include the entire IPv6 header chain are anyway unlikely to survive in real networks. Whilst currently legitimate from a specifications standpoint, they are virtually impossible to police with state-less filters and firewalls, and are hence likely to be blocked by such filters and firewalls.

This filtering policy assumes that host implementations require the Hop Limit of Neighbor Discovery messages to be 255, and discard those packets otherwise.

The aforementioned filtering rules implicitly handle the case of fragmented packets: if the ND-Shield device fails to identify the upper-layer protocol as a result of the use of fragmentation, the corresponding packets would be dropped.

Finally, we note that IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [RFC5722]) might still be subject of NS-based attacks. However, a recent assessment of IPv6 implementations [SI6-FRAG] with respect to their fragment reassembly policy seems to indicate that most current implementations comply with [RFC5722].

5.3. Filtering Neighbor Advertisement Messages

1. If the Hop Limit is not 255, pass the packet.

   Section 7.1.2 of [RFC4861] requires nodes to discard Neighbor Advertisement messages if their Hop Limit is not 255.

2. Try to identify whether the packet is an ICMPv6 Neighbor Advertisement message, by parsing the IPv6 header chain. When doing so, enforce a limit on the maximum number of Extension Headers that is allowed for each packet, and if such limit is hit before the upper-layer protocol is identified, drop the packet.

   [RFC6564] specifies a uniform format for IPv6 Extension Header, thus meaning that an IPv6 node should be able to parse an IPv6 header chain even if it contains Extension Headers that are not currently supported by that node.

3. If ND-Shield is unable to identify whether the packet is an ICMPv6 Neighbor Advertisement message or not (i.e., the packet is a first-fragment, and the necessary information is missing), drop the packet.

   Note: This rule should only be applied to non-fragmented IPv6 datagrams and IPv6 fragments with a Fragment Offset of 0 (non-first fragments can be safely passed, since they will never reassemble into a complete datagram if they are part of a Neighbor Advertisement which, according to the information it conveys and the port where it was received, should not allowed).

4. If the packet is identified to be an ICMPv6 Neighbor Advertisement message, then proceed as follows:

   1. If the Target Address is the unspecified address (::), the loopback address (::1), or a multicast address, drop the

packet.

2. If the Target Address is a unicast address not known to be in use at any of the layer-2 ports, record the Target Address as being in use on the received port, and pass the packet as usual.

3. If the Target Address is a unicast address known to be in use on a layer-2 port other than the one on which the packet was received, drop the received packet.

5. In all other cases, pass the packet as usual.

Note: For the purpose of enforcing the ND-Shield filtering policy, an ESP header [RFC4303] should be considered to be an "upper-layer protocol" (that is, it should be considered the last header in the IPv6 header chain). This means that packets employing ESP would be passed by the ND-Shield device to the intended destination. If the destination host does not have a security association with the sender of the aforementioned IPv6 packet, the packet would be dropped. Otherwise, if the packet is considered valid by the IPsec implementation at the receiving host and encapsulates a Neighbor Advertisement message, it is up to the receiving host what to do with such packet.

If a packet is dropped due to this filtering policy, then the packet drop event SHOULD be logged. The logging mechanism SHOULD include a drop counter dedicated to ND-Shield packet drops.

In order to protect current end-node IPv6 implementations, Rule #1 has been defined as a default rule to drop packets that cannot be positively identified as not being Neighbor Advertisement (NA) messages (possibly because the packet contains fragments that do not contain the entire IPv6 header chain). This means that, at least in theory, ND-Shield could result in false-positive blocking of some legitimate non-NA packets that could not be positively identified as being non-NA. In order to reduce the likelihood of false positives, Rule #1 requires that packets that would not pass the required validation checks for NA messages (Section 7.1.2 of [RFC4861]) be passed without further inspection. In any case, as noted in [I-D.gont-6man-oversized-header-chain], IPv6 packets that fail to include the entire IPv6 header chain are anyway unlikely to survive in real networks. Whilst currently legitimate from a specifications standpoint, they are virtually impossible to police with state-less filters and firewalls, and are hence likely to be blocked by such filters and firewalls.

This filtering policy assumes that host implementations require the

Hop Limit of Neighbor Discovery messages to be 255, and discard those packets otherwise.

The aforementioned filtering rules implicitly handle the case of fragmented packets: if the ND-Shield device fails to identify the upper-layer protocol as a result of the use of fragmentation, the corresponding packets would be dropped.

Finally, we note that IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [RFC5722]) might still be subject of NA-based attacks. However, a recent assessment of IPv6 implementations [SI6-FRAG] with respect to their fragment reassembly policy seems to indicate that most current implementations comply with [RFC5722].

5.4. Filtering ICMPv6 Redirect messages

This section specifies the filtering rules for ICMPv6 Redirect messages that must be implemented as part of an "ND-Shield" implementation. The aforementioned rules should be enforced on all layer-2 ports EXCEPT those that have been configured for router use.

NOTE: If ND-Shield is implemented along RA-Guard, the aforementioned configuration information will be readily available. That is, the filtering rules specified in this section should be enforced on all layer-2 ports except those that have been configured for router use.

1. If the IPv6 Source Address of the packet is not a link-local address (fe80::/10), pass the packet.

   Section 8.1 of [RFC4861] requires nodes to discard ICMPv6 Redirect messages if their IPv6 Source Address is not a link-local address.

2. If the Hop Limit is not 255, pass the packet.

   Section 8.1 of [RFC4861] requires nodes to discard ICMPv6 Redirect messages if their Hop Limit is not 255.

3. Try to identify whether the packet is an ICMPv6 Redirect message, by parsing the IPv6 header chain. When doing so, enforce a limit on the maximum number of Extension Headers that is allowed for each packet, and if such limit is hit before the upper-layer protocol is identified, drop the packet.

[RFC6564] specifies a uniform format for IPv6 Extension Header, thus meaning that an IPv6 node should be able to parse an IPv6 header chain even if it contains Extension Headers that are not currently supported by that node.

4. If ND-Shield is unable to identify whether the packet is an ICMPv6 Redirect message or not (i.e., the packet is a first-fragment, and the necessary information is missing), drop the packet.

   Note: This rule should only be applied to non-fragmented IPv6 datagrams and IPv6 fragments with a Fragment Offset of 0 (non-first fragments can be safely passed, since they will never reassemble into a complete datagram if they are part of a ICMPv6 Redirect message received on a port where such packets are not allowed).

5. If the packet is identified to be an ICMPv6 Redirect message, drop the packet.

6. In all other cases, pass the packet as usual.

Note: For the purpose of enforcing the ND-Shield filtering policy, an ESP header [RFC4303] should be considered to be an "upper-layer protocol" (that is, it should be considered the last header in the IPv6 header chain). This means that packets employing ESP would be passed by the ND-Shield device to the intended destination. If the destination host does not have a security association with the sender of the aforementioned IPv6 packet, the packet would be dropped. Otherwise, if the packet is considered valid by the IPsec implementation at the receiving host and encapsulates a ICMPv6 Redirect message, it is up to the receiving host what to do with such packet.

If a packet is dropped due to this filtering policy, then the packet drop event SHOULD be logged. The logging mechanism SHOULD include a drop counter dedicated to ND-Shield packet drops.

In order to protect current end-node IPv6 implementations, Rule #4 has been defined as a default rule to drop packets that cannot be positively identified as not being ICMPv6 Redirect messages (possibly because the packet contains fragments that do not contain the entire IPv6 header chain). This means that, at least in theory, ND-Shield could result in false-positive blocking of some legitimate non-Redirect packets that could not be positively identified as being non-Redirect. In order to reduce the likelihood of false positives, Rule #1 and Rule #2 require that packets that would not pass the required validation checks for Redirect messages (Section 8.1 of

[RFC4861]) be passed without further inspection. In any case, as noted in [I-D.gont-6man-oversized-header-chain], IPv6 packets that fail to include the entire IPv6 header chain are anyway unlikely to survive in real networks. Whilst currently legitimate from a specifications standpoint, they are virtually impossible to police with state-less filters and firewalls, and are hence likely to be blocked by such filters and firewalls.

This filtering policy assumes that host implementations require that the IPv6 Source Address of ICMPv6 Redirect messages be a link-local address, and that they discard the packet if this check fails, as required by the current IETF specifications [RFC4861]. Additionally, it assumes that hosts require the Hop Limit of Neighbor Discovery messages to be 255, and discard those packets otherwise.

The aforementioned filtering rules implicitly handle the case of fragmented packets: if the ND-Shield device fails to identify the upper-layer protocol as a result of the use of fragmentation, the corresponding packets would be dropped.

Finally, we note that IPv6 implementations that allow overlapping fragments (i.e. that do not comply with [RFC5722]) might still be subject of Redirect-based attacks. However, a recent assessment of IPv6 implementations [SI6-FRAG] with respect to their fragment reassembly policy seems to indicate that most current implementations comply with [RFC5722].

6. Security Considerations

This document specifies ND-Shield, an operational mitigation for attack vectors based on Router Solicitation, Neighbor Solicitation, Neighbor Advertisement, and Redirect messages.

We note that if an attacker sends a fragmented Neighbor Discovery packets that are deemed as 'inappropriate' by the ND-Shield device, the first-fragment would be dropped, and the rest of the fragments would be passed. This means that the victim node would tie memory buffers for the aforementioned fragments, which would never reassemble into a complete datagram. If a large number of such packets were sent by an attacker, and the victim node failed to implement proper resource management for the fragment reassembly buffer, this could lead to a Denial of Service (DoS). However, this does not really introduce a new attack vector, since an attacker could always perform the same attack by sending forged fragmented datagrams in which at least one of the fragments is missing. [CPNI-IPv6] discusses some resource management strategies that could be implemented for the fragment reassembly buffer.

Finally, we note that the most effective and efficient mitigation for these attacks would be to prohibit the use of IPv6 fragmentation with all Neighbor Discovery messages (as proposed by [I-D.gont-6man-nd-extension-headers]), such that the ND-Shield functionality is easier to implement. However, since such mitigation would require an update to existing implementations, it cannot be relied upon in the short or near term.

7. Acknowledgements

The author would like to thank Ran Atkinson, Karl Auer, Robert Downie, Washam Fan, David Farmer, Marc Heuse, Nick Hilliard, Ray Hunter, Joel Jaeggli, Simon Perreault, Arturo Servin, Gunter van de Velde, James Woodyatt, and Bjoern A. Zeeb, who provided valuable comments on the document "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)" [I-D.ietf-v6ops-ra-guard-implementation], on which this document is heavily based.

8. References

8.1. Normative References

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

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

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

[RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, December 2009.

[RFC6564] Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., and M. Bhatia, "A Uniform Format for IPv6 Extension Headers", RFC 6564, April 2012.

8.2. 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.

[I-D.gont-opsec-dhcpv6-shield] Gont, F., "DHCPv6-Shield: Protecting Against Rogue DHCPv6 Servers", draft-gont-opsec-dhcpv6-shield-00 (work in progress), May 2012.

[I-D.ietf-v6ops-ra-guard-implementation] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", draft-ietf-v6ops-ra-guard-implementation-04 (work in progress), May 2012.

[I-D.gont-6man-oversized-header-chain] Gont, F. and V. Manral, "Security and Interoperability Implications of Oversized IPv6 Header Chains", draft-gont-6man-oversized-header-chain-01 (work in progress), April 2012.

[I-D.gont-6man-nd-extension-headers]

Gont, F., "Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery", draft-gont-6man-nd-extension-headers-02 (work in progress), January 2012.

[SI6-FRAG]
SI6 Networks, "IPv6 NIDS evasion and improvements in IPv6 fragmentation/reassembly", 2012, <http://blog.si6networks.com/2012/02/ipv6-nids-evasion-and-improvements-in.html>.

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

[ARP-VULN]
Bekeey, M., "ARP Vulnerabilities: Indefensible Local Network Attacks?", Black Hat Briefings '01, 2001, <http://www.blackhat.com/presentations/bh-usa-01/MikeBeekey/bh-usa-01-Mike-Beekey.ppt>.

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

[rafixd] "rafixd", <http://www.kame.net/dev/cvsweb2.cgi/kame/kame/kame/rafixd/>.

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

[THC-IPV6]
"The Hacker's Choice IPv6 Attack Toolkit", <http://www.thc.org/thc-ipv6/>.

Appendix A. Assessment tools

UK CPNI (http://www.cpni.gov.uk) has produced assessment tools (which have not yet been made publicly available) to assess IPv6 implementations with respect to the issues described in this document. If you think that you would benefit from these tools, we might be able to provide a copy of the tools (please contact Fernando Gont at fernando@gont.com.ar).

[THC-IPV6] is a publicly-available set of tools that implements some (if not all) of the techniques described in this document.

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