Security Implications of the Use of IPv6 Extension Headers with IPv6 Neighbor Discovery (draft-gont-v6ops-ra-guard-evasion)

Arturo Servín
LACNIC

81st IETF Meeting, Quebec, Canada
July 24-29, 2011

Problem Statement

- No current use of IPv6 extension headers with ND
- However, nodes still required to suport them
- Ext. Hdrs. increase the complexity of ND control/monitoring (RA-Guard, NDPMon, etc):
  - The whole IPv6 header chain needs to be parsed
  - Fragmentation makes the life of these devices painful
    - Unless they reassemble, they can be trivially evaded/circumvented
    - Even with reasembly, control/monitoring is unreliable
    - Fragment reassembly is complex and stateful -- introduces other attack vectors!

Example: RA-Guard evasion

- RA-Guard specified in RFC 6105
- Protects a network from Rogue RAs, by filtering at layer-2 with different criteria (e.g., “allowed ports” on a switch).
- In many cases RA-Guard has been deployed and seen as a security mechanism
- Very trivial to evade with IPv6 Extension Headers, though

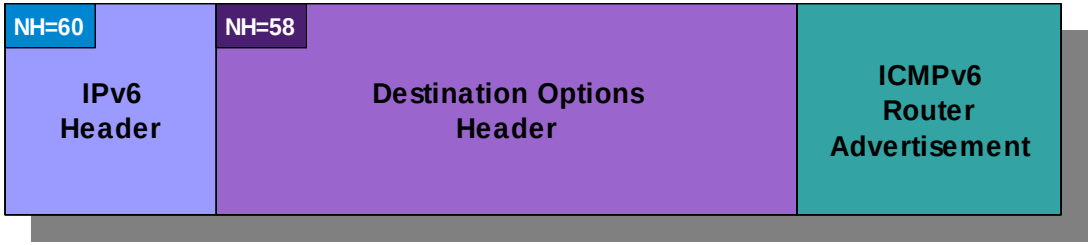
RA-Guard: Evasion technique #1

- RA-Guard implementations fail to process the entire IPv6 header chain

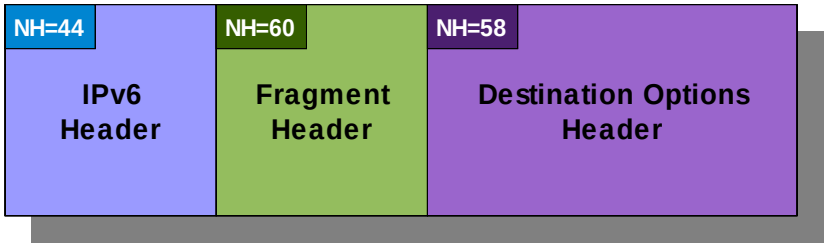
RA-Guard: Evasion technique #2

- Combination of a Destination Options Header and fragmentation:

Original Packet

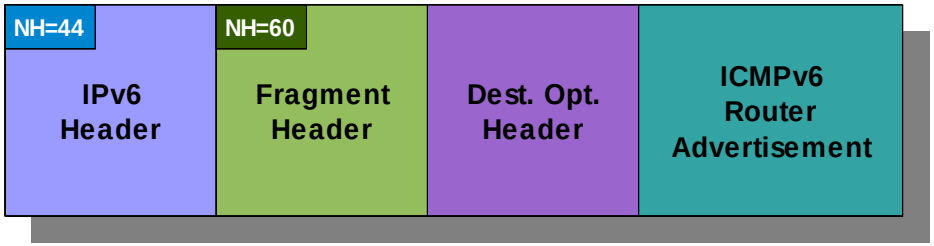


First Fragment



Can only tell there's ICMV6 inside

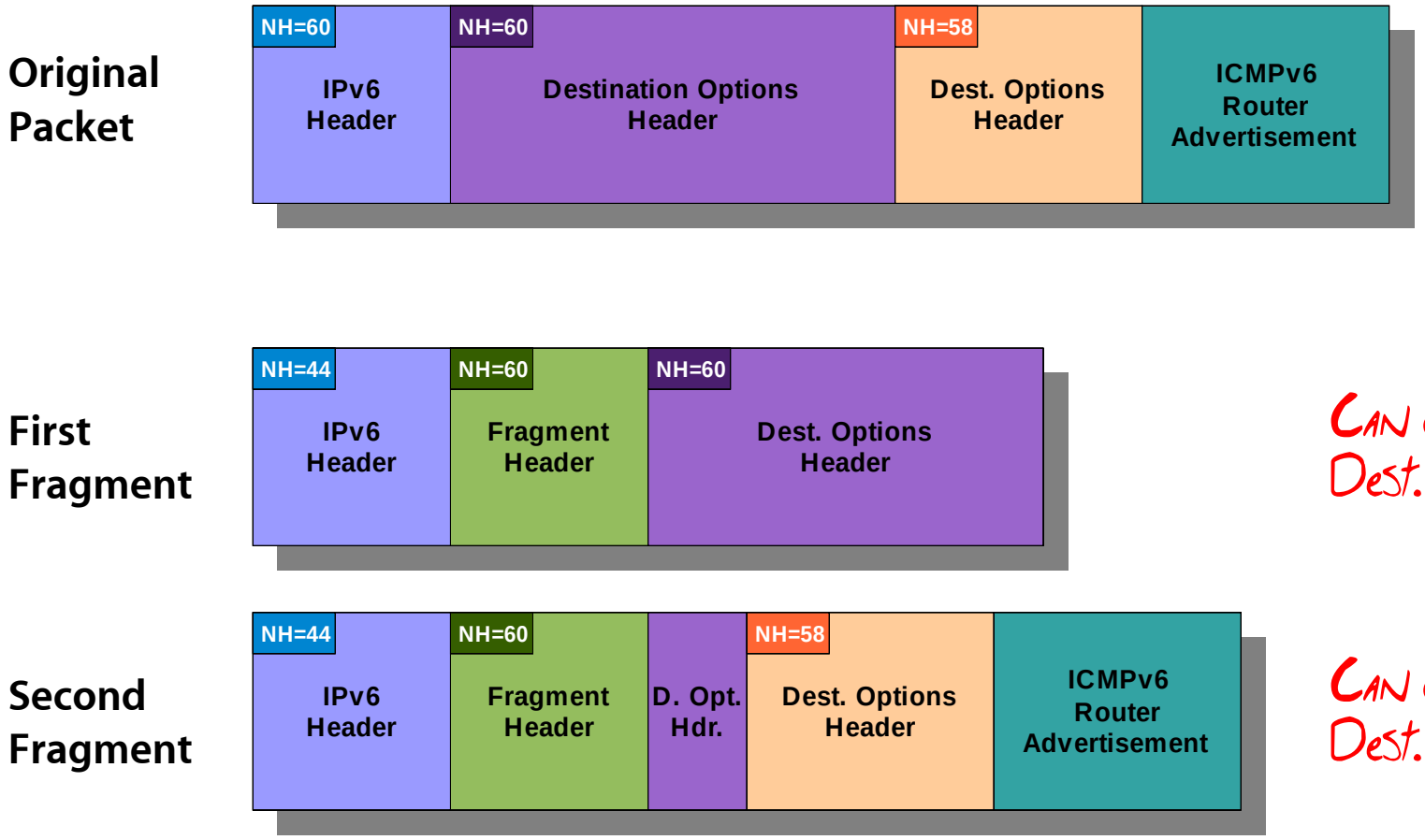
Second Fragment



Can only tell there's Dest. Opt. Hdr inside!

RA-Guard: Evasion technique #2(++)

- Two Destination Options headers, and fragmentation:



draft-gont-6man-nd-extension-headers

- Originally meant to prohibit use of all IPv6 Extension Headers with Neighbor Discovery
- This would greatly simplify ND control and monitoring

However...

- Discussion on the 6man mailing-list seemed to converge to:
  - Prohibiting IPv6 Fragment Header with IPv6
  - Allowing other Extension Headers (for possible/potential future uses)
- Conclusion seems to be:
  - Parsing the IPv6 header chain is not seen as a (hardware-wise) show-stopper
  - Fragmentation is understood to be painful for ND monitoring/control

Moving forward...

Comments?

Adopt this I-D as a v6ops wg item?