IPv6 Router Advertisement Guard (Ra-Guard) evasion

draft-gont-v6ops-ra-guard-evasion

Arturo Servín
LACNIC

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

Introduction

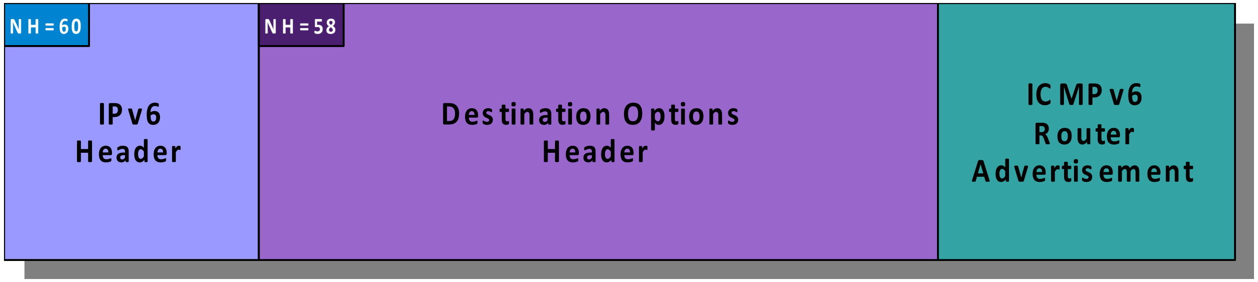
- **RFC 6104 introduces the problem statement of Rogue RAs**
  - **Focuses on misconfigured routers**
  - **Mentions different filtering criteria for filtering**
  - **Most basic filtering criterion based on the incomming port for the RA**
- **RFC 6105 specifies RA-Guard**
  - **Focuses on malicious routers (security)**
  - **Very brief Security Considerations section**
- **In many cases RA-Guard has been deployed and seen as a security mechanism**
- **It is a desired feature, since it parallells the DHCPv4-snooping of the IPv4 world**

draft-gont-v6ops-ra-guard-evasion

- **Describes RA-Guard evasion techniques**
- **Describes more advanced filtering to mitigate them (operational mitigation)**
- **Formally updates RFC 6105 -> the RA-Guard spec is updated such that these issues are addressed**
  - **Enhances the Security Considerations**
  - **Mitigates RA-Guard evasion tehniques**

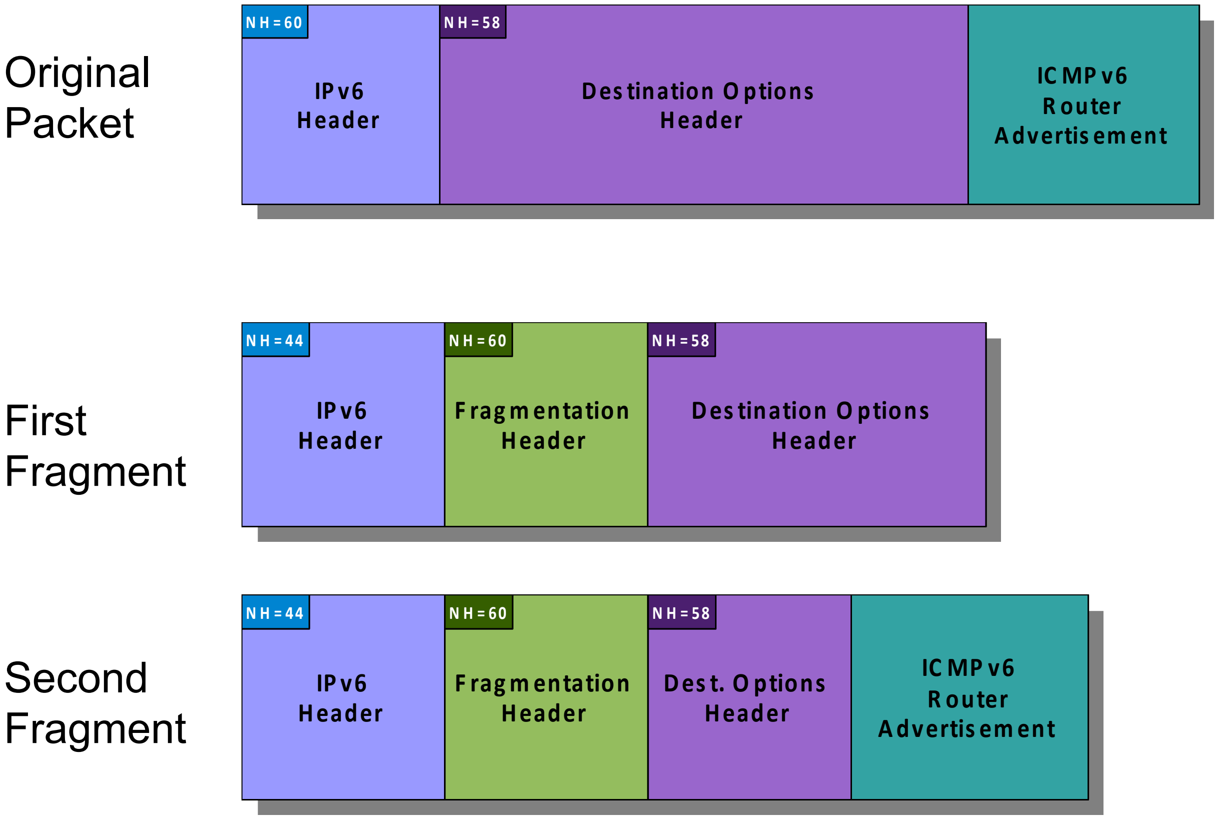
Evasion technique #1

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



Evasion technique #2

- **Combination of a Destination Options header and fragmentation:**



Original Packet

NH=60 IPv6 Header

NH=58 Destination Options Header

ICMPv6 Router Advertisement

First Fragment

NH=44 IPv6 Header

NH=60 Fragmentation Header

NH=58 Destination Options Header

Second Fragment

NH=44 IPv6 Header

NH=60 Fragmentation Header

NH=58 Dest. Options Header

ICMPv6 Router Advertisement

Mitigation:

How to filter RAs:

- **Follow the entire IPv6 header chain (possibly enforcing a limit on number of Ext. Headers) -- drop the packet if it is an RA or the Ext. Header limit is hit.**
- **If the upper layer protocol is not found (e.g. the packet is fragmented), and the IPv6 Src. Addr. is a link-local address, drop the packet ¥**
- **Else, forward the packet**

¥: RAs are required to use a link-local address

Discussion on the v6ops mailing-list

- **Was mostly focused on draft-gont-6man-nd-extension-headers**
  - □ **Related I-D about prohibiting the use of some Ext. Headers with ND**
- **There seemed to be general agreement that these evasion techniques can be mitigated as proposed**
- **Moving forward:**

Adopt this I-D as a v6ops wg item?