Security Implications of the Use of IPv6 Extension Headers with Neighbor Discovery (draft-gont-6man-nd-extension-headers)

Fernando Gont
on behalf of
UK CPNI

IETF 83
Problem statement

- IPv6 fragmentation is not necessary for ND
  - Need to send lots of options? – Send it in multiple RAs!
- Use of fragmentation prevents feature parity with IPv4
  - It makes ND-monitoring (NDMon, etc.) impossible
  - Makes mitigation of ND-based attacks difficult
- In the case of SEND,
  - You **may** need it
  - But certainly you don't want to be in that position :-(
draft-gont-6man-nd-extension-headers

- Forbids use of IPv6 fragmentation with traditional Neighbor Discovery
- Notes that in the case of SEND:
  - You may explicitly enable IPv6 fragmentation
  - Relying on IPv6 fragmentation is a bad idea
Recap of the discussion

- Document received its share of discussion on-list
- There seemed to be consensus on forbidding IPv6 fragmentation with traditional ND
- It was argued that the document needed to discuss use of IPv6 fragmentation with SEND
  - The current version of the I-D does that!
Moving forward

- Adopt this document as a 6man wg item?
Feedback?

Fernando Gont
fgont@si6networks.com