Detection of IPv6 Neighbor Discovery and Host Redirection Spoofing

draft-pashby-ipv6-detecting-spoofing-00.txt

Ron Pashby – Bowhead

Purpose

- Provide the ability to detect Neighbor Discovery and Host Redirect security breaches, by requiring:
  - Neighbor Advertisements be sent to host's Solicited Node Multicast address
  - Host Redirects be sent to host's Solicited Node Multicast address

Justification

- Well known attacks (even in IPv4)
- There was no way to detect in IPv4
- Duplicate Detection is mandatory in IPv6 and was optional in IPv4
- Only way to block Host Redirect was to disable it at the host level
- IPv6 has a mechanism that would easily allow for detection

Changes to Neighbor Discovery

- Neighbor Advertisement (NA) messages shall be sent to host’s Solicited-node Multicast Address (SMA)
- Silently discard NA messages that were received via non-SMA address (Optionally may accept for backward compatibility)
- Host Redirect (HR) messages shall be sent to host’s SMA
- Silently discard HR messages that were received via non-SMA address (Optionally may accept for backward compatibility)

Related Drafts

draft-pashby-mboned-mc-scoped-addr

- "Multicast Scoped Address Assignment Guidence"
- Defines Dynamically Assigned Link-Local Scoped multicast Id range (SMAs are included in this range)

draft-pashby-magma-simplify-mld-snooping

- "Simplifying IPv6 MLD Snooping Switches"
- Recommends Dynamically Assigned Link-Local Scoped be sent to all ports without the need for MLD Joins and MLD state for these groups

Recommendation

- Accept this draft as a WG draft and proceed to incorporate modifications into RFC2461

Questions?