Validating the IPv6 ND SLLA and TLLA Options

draft-gont-6man-lla-opt-validation-00

Fernando Gont
Ron Bonica
Will (Shucheng) Liu

Background

- IPv6 nodes maintain a neighbor cache
  - Each cache entry represents an on-link neighbor
  - Each cache entry maps the neighbor's IP address to a link-layer address
- IPv6 nodes populate one other's neighbor cache by exchanging IPv6 ND messages
- IPv6 nodes can craft ND messages that poison one another's neighbor cache

Two ND-Based Attacks

- Cause the victim to map the IP address of an on-link neighbor to one of its own link layer addresses
  - Causes routing loops when the victim is a router
- Cause the victim to map the IP address of an on-link neighbor to a link layer broadcast or multicast address
  - Causes routing loops when victim is a router
  - Causes unintended forwarding behaviors

Advice

- Avoid sharing links with non-trusted parties
- However, some scenarios requires such sharing
  - Public access
  - Compromised neighbors
- So, validate ND messages to the greatest degree possible

Proposed Validation Rules

- IPv6 nodes MUST execute the following validation checks on incoming ICMPv6 messages
  - SLLA and TLLA options MUST NOT contain a link-layer address that is local to the recipient
  - SLLA and TLLA options MUST NOT contain a broadcast or multicast link layer address
- IPv6 nodes MUST discard ICMPv6 packets that do not conform to the above-mentioned rules

Ask

- Review draft
- Comment on list
- Adopt as WG draft by IETF 90