# ND-Shield: Protecting against Neighbor Discovery Attacks

## (draft-gont-opsec-nd-shield)

**Fernando Gont**

SI6 NETWORKS

IETF 84
Vancouver, Canada. July 29-August 3, 2012

# Overview

- Aims at blocking Neighbor Discovery attacks at the link-layer
- It targets attack vectors based on:
    - Neighbor Solicitation
    - Neighbor Advertisement
    - Router Solicitation
    - Redirect messages
- **Complements other technologies such as RA-Guard**
    - Even if you do RA-Guard, an attacker can still become the “Next-Hop Router” by sending other non-RA Neighbor Discovery packets

# draft-gont-opsec-nd-shield

- Specifies the filtering rules for ND-Shield, i.e., how to filter:
  - Neighbor Solicitations
  - Neighbor Advertisements
  - Router Solicitations
  - Redirects
- Greatly benefits from work done in v6ops for RA-Guard

# Filtering rules

General rules for all messages:

1. Follow the entire IPv6 header chain to identify the type of packet
2. If the packet is a first-fragment and the upper-layer header is not found, drop the packet
3. If the Source Address had not been previously seen, record the address, otherwise filter the packet if it has been received on a different port
4. [Type-specific filtering]
5. Otherwise, pass the packet as usual

# Open issues

- Current I-D specifies the rules on a per-packet-type basis
- Might want to coalesce all filtering rules
  - Probably more useful from an implementor's point of view

# Moving forward

- Adopt as an OPSEC WG item?

# Thanks!

Fernando Gont

fgont@si6networks.com

www.si6networks.com