LISP Threats Analysis

draft-ietf-lisp-threats-11 (Dec.)
draft-ietf-lisp-threats-12 (Mar.)

- Editorial polishing.

- Clarifications added in few points.

-12

- Editorial polishing.
- Address general comments from mailing list.
- Add a threats mitigation section.

Mitigations

Be rigorous

- Most threats can be mitigated with
  - filters and rate limitations,
  - configurations verifications,
  - deactivation of features that are not absolutely required.

Authenticate control-plane messages

- Always use the authentication mechanisms provided in the specifications

  - for Map-Request/Map-Reply/Map-Register see RFC6830, RFC6833 and LISP-Sec;

  - for messages exchanged internally in the mapping system see LISP-DDT.

- The *authentication data field* specified in RFC6830 permits to generalise authentication to all mapping system messages.

Slow-down attackers

- Rate limit control-plane actions triggered by data-plane events.

Verify information

- Never directly use non-solicited informations (unless authenticated)

- use them as hints to trigger a trustable information retrieval.

Last call?