Update on LISP Threats Analysis

~~draft-saucez-lisp-security-01.txt~~
~~draft-saucez-lisp-security-02.txt~~
~~draft-saucez-lisp-security-03.txt~~
~~draft-ietf-lisp-threats-00.txt~~
~~draft-ietf-lisp-threats-01.txt~~
~~draft-ietf-lisp-threats-02.txt~~
~~draft-ietf-lisp-threats-03.txt~~
draft-ietf-lisp-threats-04.txt

Damien Saucez
Luigi Iannone
Olivier Bonaventure

Main changes -03

- Clearly specify that the document is related to public deployment of LISP
- Addition of a severity level discussion at the end of each threat

Severity Level

- How harmful is a threat? How easy is it to neutralize it?
- LISP can be put at the same threat level as current Internet by configuration and good deployment

Severity Level (contd.)

- **Level 0**: equivalent to the risk without LISP
- **Level 1**: can be neutralized by configuration and deployment
- **Level 2**: can be neutralized by deactivating the feature without loosing functionality
- **Level 3**: cannot be neutralized without changing LISP specification or architecture

Level 0
(no additional threat)

- 5.1. EID-to-RLOC Database Threats
- 7. Threats concerning Interworking

Level 1
(neutralized with config/deployment)

- 5.3. Attacks not leveraging on the LISP header
- 5.4.2. Attacks using the Map-Version bit
- 5.4.4. Attacks using the Instance ID bits
- 6.1. Attacks with Map-Request messages
- 6.2. Attacks with Map-Reply messages
- 9.1. LISP+ALT / 9.2. LISP-DDT
- 10.1. Map Server / 10.2. Map Resolver

➡ **Anti-spoof + rate limiting + appropriate configuration**

Level 2
(neutralized by deactivation)

- 5.4.1. Attacks using the Locator Status Bits
- 5.4.3. Attacks using the Nonce-Present and the Echo-Nonce bits
- 6.1. appending Map-Records to Map-Request messages
- 6.3. Gleaning Attacks
- 8. Threats with Malicious xTRs

Level 3
(need changing LISP)

- We found no threat on public LISP deployment that couldn't be solved with configuration of deactivation

Summary

- **Careful configuration and deployments gives similar threats level as today's Internet**
- Clear statement that the document compares threats of public LISP deployments with threats in the current Internet architecture
- Addition of a severity level discussion at the end of each section
- Addressed comments from D. Lewis' and V. Ermagan reviews
- Updated References
- Further editorial polishing

Next Steps...

- Is severity the best word?
- Do people agree with proposed severity levels?
- Is the document ready for last-call?