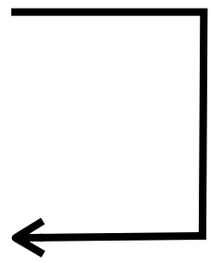
Update on LISP Threats Analysis

~~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-03.txt~~
~~draft-ietf-lisp-threats-04.txt~~
~~draft-ietf-lisp-threats-05.txt~~
~~draft-ietf-lisp-threats-06.txt~~
~~draft-ietf-lisp-threats-07.txt~~
draft-ietf-lisp-threats-08.txt



Damien Saucez
Luigi Iannone
Olivier Bonaventure

Changes since IETF86

-05:

- removal of severity levels

-06:

- complete restructuration, temporary version to be used at interim meeting

-07:

- changes according to the thorough review made at interim meeting
- brief recommendations put in the security consideration section
- editorial polishing

-08:

- addition of a privacy consideration note
- editorial polishing

Structure simplification

Attack vectors vs attack categories

- Attack vectors:
  - describes techniques to build attacks
- Attack categories:
  - describes the possible attacks
    - for each category, list of vectors to succeed the attack
- No attack receipt anymore
- No specific recommendation anymore

Attack categories

- Intrusion
  - attackers gain remote access to a network they are not allowed to access normally
- Denial of Service (DoS)
  - attackers make their target unable to operate properly
- Subversion
  - attackers gain access to sensitive information (e.g., eavesdropping)

Last call?