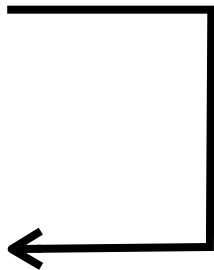


Update on LISP Threats Analysis

~~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 restructuring, 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

1. Introduction	3
2. Definition of Terms	4
3. On-path Attackers	4
4. Off-Path Attackers: Reference Environment	4
5. Data-Plane Threats	6
5.1. EID-to-RLOC Database Threats	6
5.2. EID-to-RLOC Cache Threats	7
5.2.1. EID-to-RLOC Cache poisoning	7
5.2.2. EID-to-RLOC Cache overflow	9
5.3. Attacks not leveraging on the LISP header	9
5.4. Attacks leveraging on the LISP header	10
5.4.1. Attacks using the Locator Status Bits	10
5.4.2. Attacks using the Map-Version bit	11
5.4.3. Attacks using the Nonce-Present and the Echo-Nonce bits	12
5.4.4. Attacks using the Instance ID bits	14
6. Control Plane Threats	14
6.1. Attacks with Map-Request messages	14
6.2. Attacks with Map-Reply messages	16
6.3. Gleaning Attacks	17
7. Threats concerning Interworking	18
8. Threats with Malicious xTRs	19
9. Security of the Proposed Mapping Systems	22
9.1. LISP+ALT	22
9.2. LISP-DDT	24
10. Threats concerning LISP-MS	25
10.1. Map Server	25
10.2. Map Resolver	26
11. Security Recommendations	27
12. IANA Considerations	30
13. Security Considerations	30
14. Acknowledgments	30
15. References	30
15.1. Normative References	30
15.2. Informative References	31
Appendix A. Document Change Log	32
Authors' Addresses	33

1. Introduction	2
2. On-path Attackers	3
3. Off-Path Attackers: Reference Environment	4
4. Attack vectors	5
4.1. Configured EID-to-RLOC mappings	5
4.2. EID-to-RLOC Cache	6
4.3. Attacks using the data-plane	6
4.3.1. Attacks not leveraging on the LISP header	6
4.3.2. Attacks leveraging on the LISP header	8
4.4. Attacks using the control-plane	11
4.4.1. Attacks with Map-Request messages	11
4.4.2. Attacks with Map-Reply messages	12
4.4.3. Attacks with Map-Register messages	13
4.4.4. Attacks with Map-Notify messages	14
5. Attack categories	14
5.1. Intrusion	14
5.1.1. Description	14
5.1.2. Vectors	14
5.2. Denial of Service (DoS)	14
5.2.1. Description	14
5.2.2. Vectors	15
5.3. Subversion	15
5.3.1. Description	15
5.3.2. Vectors	15
6. Note on privacy	16
7. IANA Considerations	16
8. Security Considerations	16
9. Acknowledgments	17
10. References	17
10.1. Normative References	17
10.2. Informative References	18
Appendix A. Document Change Log	19
Authors' Addresses	21

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?