

# LISP Threats Analysis

## draft-ietf-lisp-threats-10

Damien Saucez  
IETF 90

# Changelog

- Document completely restructured
- Remove all assumptions (e.g., on-path attackers are taken into account)
- Distinction between modes of operation, threat categories, and attack vectors

# Document completely restructured

- To avoid becoming a receipt of attacks, they are abstracted in the threat model
  - Attacker modes of operation
    - where are located attackers?
  - Threat categories
    - what is the purpose of the attack?
- Then list the categories of threats doable for each LISP feature and using what mode

# Table of Contents

1. Introduction . . . . .	3
2. <del>On-path Attackers</del> Threat model . . . . .	3
<del>3. Off-Path Attackers; Reference Environment</del>	
2.1. Attacker modes of operation . . . . .	3
<del>4. Attack vectors . . . . .</del>	4
2.1.1. On-path attackers vs. Off-path attackers . . . . .	4
2.1.2. Internal attackers vs. External attackers . . . . .	4
2.1.3. Live attackers vs. Time-shifted attackers . . . . .	4
2.1.4. Control-plane attackers vs. Data-plane attackers . . . . .	5
<del>4.1. Configured EID-to-RISE mappings</del>	
2.1.5. Cross mode attackers . . . . .	6
<del>4.2. EID-to-RISE Cache . . . . .</del>	5
2.2. Threat categories . . . . .	6
<del>4.3. Attacks using the data-plane . . . . .</del>	5
2.2.1. Replay attack . . . . .	7
<del>4.3.1. Attacks not leveraging on the LISP header . . . . .</del>	7
<del>4.3.2. Attacks leveraging on the LISP header . . . . .</del>	5
2.2.2. Packet manipulation . . . . .	8
<del>4.4. Attacks using the control-plane . . . . .</del>	5
2.2.3. Packet interception and suppression . . . . .	11
<del>4.4.1. Attacks with Map-Request messages . . . . .</del>	6
2.2.4. Spoofing . . . . .	11
<del>4.4.2. Attacks with Map-Reply messages . . . . .</del>	12
<del>4.4.3. Attacks with Map-Register messages . . . . .</del>	13
<del>4.4.4. Attacks with Map-Notify messages . . . . .</del>	6
2.2.5. Rogue attack . . . . .	14
<del>5. Attack categories . . . . .</del>	6
2.2.6. Denial of Service (DoS) attack . . . . .	7
2.2.7. Performance attack . . . . .	14
<del>5.1. . . . .</del>	7
2.2.8. Intrusion attack . . . . .	7
2.2.9. Amplification attack . . . . .	14
<del>5.1.1. Description . . . . .</del>	7
2.2.10. Multi-category attacks . . . . .	14
<del>5.1.2. Vectors . . . . .</del>	7
3. Attack vectors . . . . .	14
<del>5.2. Denial of Service (DoS) . . . . .</del>	7
3.1. Gleaning . . . . .	14
<del>5.2.1. Description . . . . .</del>	7
3.2. Locator Status Bits . . . . .	14
<del>5.2.2. Vectors . . . . .</del>	9
3.3. Map-Version . . . . .	14
<del>5.3. Subversion . . . . .</del>	9
3.4. Echo-Nonce algorithm . . . . .	15
<del>5.3.1. Description . . . . .</del>	10
3.5. Instance ID . . . . .	15
<del>5.3.2. Vectors . . . . .</del>	11
3.6. Interworking . . . . .	15
<del>6. Note on Privacy . . . . .</del>	11
3.7. Map-Request messages . . . . .	16
<del>7. IANA Considerations . . . . .</del>	12
3.8. Map-Reply messages . . . . .	16
<del>8. Security Considerations . . . . .</del>	13
3.9. Map-Register messages . . . . .	16
<del>9. Acknowledgments . . . . .</del>	14
3.10. Map-Notify messages . . . . .	16
<del>10. References . . . . .</del>	14
4. Note on Privacy . . . . .	14
5. IANA Considerations . . . . .	17
<del>10.1. Normative References . . . . .</del>	17
<del>10.2. Informative References . . . . .</del>	15
6. Security Considerations . . . . .	17
<del>Appendix A. Document Change Log . . . . .</del>	15
7. Acknowledgments . . . . .	18
<del>Authors' Addresses . . . . .</del>	15
8. References . . . . .	20

## 1. Introduction

~~The Locator/ID Separation Protocol (LISP) is specified in [RFC6830].~~  
~~The present document assesses the potential security threats identified~~  
~~in the LISP specifications if LISP is . . . . .~~

8.1. Normative References . . . . .	16
8.2. Informative References . . . . .	16
Appendix A. Document Change Log . . . . .	17
Authors' Addresses . . . . .	19

# Attacker modes of operation

- On-path attackers vs. Off-path attackers
- Internal attackers vs. External attackers
- Live attackers vs. Time-shifted attackers
- Control-plane attackers vs. Data-plane attackers
- *Cross mode attackers*

# Threat categories

- Replay attack
- Packet manipulation
- Packet interception and suppression
- Spoofing
- Rogue attack
- Denial of Service (DoS) attack
- Performance attack
- Intrusion attack
- Amplification attack
- *Multi-category attacks*

# Attack vectors

- Gleaning
- Locator Status Bits
- Map-Version
- Echo-Nonce algorithm
- Instance ID
- Interworking
- Map-Request messages
- Map-Reply messages
- Map-Register messages
- Map-Notify messages

# Solutions to defend

In the charter:

*LISP security threats and solutions: This document will describe the security analysis of the LISP system, what issues it needs to protect against, and a solution that helps defend against those issues. The replay attack problem discussed on the mailing list should be included in this work.*

What about using I.D.-threats just to list the risks and extend I.D.-lisp-sec to propose mitigations?



# LISP Threats Analysis

## draft-ietf-lisp-threats-10

Damien Saucez  
IETF 90