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

The Locator/ID Separation Protocol (LISP) is specified in [RFC6830]. The present document assess the potential security threats identified in the LISP specifications if LISP is 16

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