Network Working Group D. Saucez
Internet-Draft Universite catholique de Louvain
Intended status: Standards Track L. Iannone
Expires: April 22, 2010 TU Berlin - Deutsche Telekom
Laboratories AG
O. Bonaventure
Universite catholique de Louvain
October 19, 2009

# Notes on LISP Security Threats and Requirements
draft-saucez-lisp-security-00.txt

## Status of this Memo

## Copyright Notice

## Abstract

The present document is a preliminary collection of notes about LISP security threats and requirements. Its purpose is to start a discussion on the subject among people that have shown interest in working on the matter.

Table of Contents

## 1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

## 2. Introduction

The Locator/ID Separation Protocol (LISP) is defined in draft-ietf-lisp-05.txt [I-D.ietf-lisp]. The present document aims at identifying threats in the current LISP specification and possibly list a set of requirements or mechanism needed to improve its security. A preliminary security analysis on LISP has been conducted by M. Bagnulo in [I-D.bagnulo-lisp-threat].

This document is split in two main parts; one concerning the data-plane and one concerning the control-Plane.

The LISP data-plane consists of LISP packet encapsulation, decapsulation, and forwarding and includes the LISP-Cache and LISP-Database data structures used to perform these operations. The present document will try to analyze the possible threats of the data-plane.

The LISP control-plane consists in the mapping distribution system, which can be one of the mapping distribution protocols proposed so far (e.g., [I-D.ietf-lisp-ms], [I-D.ietf-lisp-alt], [I-D.meyer-lisp-cons], and [I-D.lear-lisp-nerd] ), and the set of Map-Request and Map-Reply messages. The present document will not analyze all possible threats of each specific mapping distribution protocol. Rather, this document will try to find a common set of requirements that every present and future mapping distribution protocol should satisfy in order to reduce as much as possible threats related to the LISP control-plane.

## 3. Definition of Terms

See [I-D.ietf-lisp]

## 4. Data-plane threats

This section contains some threats and attacks related to the LISP data-plane. By LISP data-plane it is intended the operations of encapsulation, decapsulation, and forwarding as well as the content of the LISP-Cache and LISP-Database as specified in the original LISP document ([I-D.ietf-lisp]).

### 4.1. Security of the data stream

In some context it could be necessary to secure the data stream that is LISP encapsulated. This can be achieved with two different approaches:

- Securing messages. In this approach a field needs to be added to the LISP header in order to secure the content.

- Securing the transport protocol. An example of this approach is the use of IPSEC to secure the content of the original, non LISP-encapsulated, packet.

What is the approach suitable in the LISP context?

### 4.2. LISP-encapsulated packet spoofing

Like any other type of packet in the Internet, LISP encapsulated packets can also be spoofed. Generally the term "spoofed packet" indicates a packet containing a source IP address which is not the one of the actual originator of the packet. Since LISP uses encapsulation, this translates in two types of spoofing:

- EID Spoofing: The originator of the packet puts in it a spoofed EID. The packet will be normally encapsulated by the ITR of the site.

- RLOC Spoofing: The originator of the packet generates directly a LISP-encapsulated packet with a spoofed source RLOC.

Note that the two types of spoofing are not mutually exclusive, rather all combinations are possible and can be used to perform several kind of attacks.

The work done in the SAVI WG ([SAVI]) can be useful in mitigating spoofing.

It is worth to notice that in the context of LISP, there is also the possibility to spoof part of the content of the LISP-specific header in order to perform some attacks. The various possibilities are listed in the following sections, while describing the possible attacks.

### 4.3. Nonce

The "Nonce" gives some basic security support by acting as a "session cookie", similar to what is used in L2TP ([I-D.ietf-l2tpext-l2tp-base]). The use of the Nonce to mitigate some of the possible attacks is described in the following sections.

There should be an explicit discussion on the limits of the Nonce?

### 4.4. LISP-Cache threats

A key component of the overall LISP architecture is the LISP-Cache. The LISP-Cache is the data structure that stores the bindings between EID and RLOC (namely the "mappings") to be used later on. Attacks against this data structure can happen either when the mappings are first installed in the cache (see also Section 5) or by corrupting (poisoning) the mappings already present in the cache.

#### 4.4.1. LISP-Cache poisoning

The content of the LISP-Cache can be poisoned by spoofing LISP encapsulated packets. Example of LISP-Cache poisoning are:

Fake mapping: The cache contains entirely fake mappings that do not originate from an authoritative mapping server. This can be achieved either through gleaning as described in Section 4.6.2 or by attacking the control-plane as described in Section 5.

EID Poisoning: The EID-Prefix in a specific mapping is not owned by the originator of the entry. Similarly to the previous case, this can be achieved either through gleaning as described in Section 4.6.2 or by attacking the control-plane as described in Section 5.

EID redirection/RLOC poisoning: The EID-Prefix in the mapping is not bound to (located by) the set of RLOCs present in the mapping. This can result in packets being redirected elsewhere, eavesdropped, or even blackholed. Note that not necessarily all RLOCs are fake/spoofed. The attack works also if only part of the RLOCs, the highest priority ones, are compromised. Again, this can be achieved either through the gleaning as described in Section 4.6.2 or by attacking the control-plane as described in Section 5.

Reachability poisoning: The reachability information stored in the mapping could be poisoned, redirecting the packets to a subset of the RLOCs (or even stopping it if locator status bits are all set to 0). If reachability information is not verified through the control-plane this attack can be simply achieved by sending a spoofed packet with swapped or all locator status bits reset. The same result can be obtained by attacking the control-plane as described in Section 5.

Traffic Engineering information poisoning: The LISP protocol defines two attributes associated to each RLOC in order to perform inbound Traffic Engineering: namely priority and weight. By injecting fake TE attributes, the attacker is able to break load balancing policies and concentrate all the traffic on a single RLOC or put more load on a RLOC than what is expected, creating congestion. Corrupting the TE attributes can be achieved by attacking the control-plane as described in Section 5.

Mapping TTL poisoning: The LISP protocol associates a Time-To-Live to each mapping that, once expired, allows to delete a mapping from the LISP-Cache (or forces a Map-Request/Map-Reply exchange to refresh it if still needed). By injecting fake TTL values, an attacker can either shrink the Cache (using very short TTL), thus creating an excess of cache miss causing a DoS on the mapping system, or it can increase the size of the cache by putting very high TTL values, up to a cache overflow (see Section 4.4.2). Corrupting the TTL can be achieved by attacking the control-plane as described in Section 5.

If the above listed attacks succeed, the attacker has the means of controlling the traffic.

### 4.4.2. LISP-Cache overflow

Depending on how the LISP-cache is managed (e.g., LRU vs. LFU) and depending on its size, an attacker can try to fill the cache with fake mappings. Once the cache is full, some mappings will be replaced by new fake ones, causing traffic disruption.

This can be achieved either through the gleaning as described in Section 4.6.2 or by attacking the control-plane as described in Section 5.

Another way to generate a LISP-Cache overflow is by injecting mapping with a fake and very large TTL value. In this case the cache will keep a large amount of mappings ending with a completely full cache. This type of attack can also be performed through the control-plane.

### 4.5. LISP-Database threats

The LISP-Database data structure is meant to contain the mappings that are "owned" locally, i.e., the mappings that are used for selecting the source RLOC when encapsulating, and binding the EID-Prefix behind the xTR and the RLOCs present on the xTR.

The simplest way to fill the LISP-Database is by configuration on each single xTR. This secure the data structure as much as the xTR itself is robust to intrusions.

Nevertheless, part of the information contained in the mappings that are in the LISP-Database are subject to change in time, e.g., reachability information, TE attributes, etc. The way mappings are updated can open security breaches allowing attackers to poison or corrupt the LISP-Database in a way similar to the LISP-Cache. These attacks are more related to the control-plane and will be discussed in Section 5.

### 4.6. DoS threats

This section tries to list all possible DoS attacks and suggests, when possible, mechanisms that help in mitigating the threat.

#### 4.6.1. Locator Status Bits

Locator Status Bits should be used only as a hint, meaning that upon reception of a packet having Locator Status Bits different from what is stored in the mapping present in the LISP-Cache, a Map-Request is issued in order to have confirmation of the change. However, with this behavior, an attacker can send a burst of packets with different locato status bits in order to trigger a burst of Map-Request packets, thus again attacking the control-plane. The echo nonce machanisme is proposed, we still have to analyze it in details. Several counter-measures can be introduced to mitigate its effects:

- Ignore Locator Status Bits if nonce does not change.

- Rate limitation can be used to reduce the number of issued Map-Request packets.

#### 4.6.2. Gleaning

Gleaning is used to install in the LISP-Cache a partial mapping created by gleaning the source EID and source RLOC from the first packet of a flow. The mapping is considered "partial" because it just associate an EID (/32) to one single RLOC, not the EID-Prefix the EID belongs to with the complete set of RLOCs. Gleaning can be used to perform several different attacks:

- LISP-Cache poisoning: an attacker can use gleaning to install fake mappings in the LISP-Cache (by spoofing the EID). See LISP-Cache poisoning in Section 4.4.1.

- LISP-Cache overflow: an attacker can use gleaning to install a large number of mappings in the LISP-Cache until filling it up. See LISP-Cache overflow in Section 4.4.2. Since the mapping installed in the LISP-Cache is not for a EID-Prefix but for a full EID, by sending a burst of packet for several different spoofed EIDs, an attacker could end up filling the Cache.

- Map-Request burst: if for each mapping installed by a gleaning a Map-Request is issued to retrieve the full mapping, an attacker can send a burst of packets with different EIDs generating a burst of Map-Request. Note that in this case, if Map-Request rate limitation is done on a per-EID basis, the attacker can easily bypass the rate limitation by putting different EIDs in the packets causing the gleaning.

Possible counter-measure to mitigate this issue:

- The LISP-Cache poisoning and overflow issues can be solved by filtering spoofed EIDs on the ITR (see Section 4.2).

- To reduce the Map-Request burst an approach is to send a Map-Request only if a certain amount of packets has been sent using the gleaned entry, as suggested in [Saucez09].

#### 4.6.3. Rate Limitation

The Rate-Limitation policy, used to reduce the effects of some types of DoS attacks can be itself used for a DoS attack. An attacker can send some fake packets in order to generate a burst of Map-Request packets that will be rate limited. When a legitimate packet generates a legitimate Map-Request, this will be delayed or dropped due to rate limitation, causing an increased latency.

- Any solution for this?

#### 4.6.4. Mapping System and Filtering

The use of some form of filtering can help in avoid or at least mitigate some types of attacks.

On ITRs, packets should be encapsulated only if the source EID is effectively part of the EID-Prefix downstream the ITR. Further, still on ITRs, packets should be encapsulated only if a mapping obtained from the mapping system is present in the LIP-Cache.

On ETRs, packets should be decapsulated only if the destination EID is effectively part of the EID-Prefix downstream the ETR. Further, still on ETRs, packets should be decapsulated only if a mapping for the source EID is present in the LISP-Cache and has been obtained through the mapping system (not gleaned).

Note that this filtering, since complete mappings need to be installed in both ITRs and ETRs, can introduce a higher connection setup latency and hence potentially more packets drops due to the lack of mappings in the LISP-Cache.

### 4.7. Other Attacks

#### 4.7.1. Time-shifted attacks

A time-shifted attack is an attack where the attacker is temporarily on the path between two communicating hosts. While it is on-path, the attacker sends specially crafted packets or modifies packets exchanged by the communicating hosts in order to disturb the flow of packets (e.g., by performing a man in the middle attack). An important issue for time shifted attacks is the duration of the attack once the attacker has left the path between the two communicating hosts.

#### 4.7.2. Amplification attacks

An amplification attack occurs when an attacker sends a small packet with a spoofed source to a host or router that replies by sending a longer packet to the spoofed source. To reduce the impact of such attacks, protocol designers try to avoid sending a long response after having received a small packet from a potentially spoofed source.

## 5. Control-plane threats

As pointed out in the previous sections, a good share of attacks can be avoided by securing the LISP control plane.

Here the focus is not to analyze the security threats of any specific mapping distribution protocol. Rather, the focus is to find a common set of requirements that existing or future mapping distribution protocols have to fulfill in order provide a sufficient level of security.

The LISP Map Server protocol will instead be analyzed since it is not related to any specific mapping distribution protocol.

Work and experience performed in the DNSSEC [RFC4033] and SIDR [SIDR] can be useful here.

### 5.1. Control-plane Requirements

- Authenticate the origin of a message.

- Identify the origin of a message.

- Prove that the mapping is generated by the owner of the EID or a third party allowed to generate such a mapping.

- Inject mappings in the mapping system only if the EID is allowed to be in the mapping system.

- Prove that the RLOCs associate to a mapping belong to the xTRs owning the mapping’s EID.

- Low message overhead.

- Low traffic overhead.

- Low time overhead (avoid multiple RTTs).

- Other?

### 5.2. LISP-Database coherence

The mappings present on the LISP-Database of the different xTRs of a site should always be coherent. An attacker should not be able to install different mappings for different xTRs.

A simple approach is to have a central authority in the site that pushes all the mappings in the xTRs. When a xTR decides to change something it informs the central authority, which will push the information to the other xTRs.

Each xTR is authoritative on the reachability of its locator. An xTR is not allowed to send updates to the central entity only if it is one of its RLOC.

The central authority knows the configuration which RLOC is owned by which xTR.

All of this does not prevent from securing the exchanges between the xTRs and the central authority in order to avoid spoofing attacks.

### 5.3. LISP Map Server

The LISP Map Server is a fundamental building block of the whole LISP architecture, providing an additional level of indirection allowing to run mapping distribution protocols on machines different from xTRs. From this point of view it can be considered a security improvement since xTR are not directly involved in the mapping distribution system.

Things to look closer:

- Threats concerning messages.

- DoS attacks.

- Threats concerning LISP Map Server with caching.

- Others?

## 6. Interaction between Data- and Control-plane

It is clear that attacks targeting the data-plane can have side-effects on the control-plane and vice-versa. Furthermore, attacks to the control-plane can be performed leveraging on the data-plane and vice-versa.

An analysis of the possible threats has been performed in the previous sections. Here we just characterize them following the above mentioned classification.

### 6.1. Data-plane side effects on the control-plane

To be done.

### 6.2. Control-plane side effects on the data-plane

To be done.

### 6.3. Data-plane threats leveraging on the control-plane

To be done.

### 6.4. Control-plane threats leveraging on the data-plane

To be done.

## 7. IANA Considerations

This document makes no request of the IANA.

## 8. Security Considerations

Security considerations are the core of this document and do not need to be further discussed in this section.

## 9. Acknowledgments

This work has been partially supported by the INFSO-ICT-216372 TRILOGY Project (www.trilogy-project.org).

## 10. Normative References

[I-D.bagnulo-lisp-threat]
Bagnulo, M., "Preliminary LISP Threat Analysis", draft-bagnulo-lisp-threat-01 (work in progress), July 2007.

[I-D.ietf-l2tpext-l2tp-base]
Lau, J., "Layer Two Tunneling Protocol (Version 3)", draft-ietf-l2tpext-l2tp-base-15 (work in progress), December 2004.

[I-D.ietf-lisp]
Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol (LISP)", draft-ietf-lisp-05 (work in progress), September 2009.

[I-D.ietf-lisp-alt]
Fuller, V., Farinacci, D., Meyer, D., and D. Lewis, "LISP Alternative Topology (LISP+ALT)", draft-ietf-lisp-alt-01 (work in progress), May 2009.

[I-D.ietf-lisp-ms]
Fuller, V. and D. Farinacci, "LISP Map Server", draft-ietf-lisp-ms-04 (work in progress), October 2009.

[I-D.lear-lisp-nerd]
Lear, E., "NERD: A Not-so-novel EID to RLOC Database", draft-lear-lisp-nerd-04 (work in progress), April 2008.

[I-D.meyer-lisp-cons]
Brim, S., "LISP-CONS: A Content distribution Overlay Network Service for LISP", draft-meyer-lisp-cons-04 (work in progress), April 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[SAVI] IETF, "Source Address Validation Improvements Working Group", <http://tools.ietf.org/wg/savi/>.

[SIDR] IETF, "Secure Inter-Domain Routing Working Group", <http://tools.ietf.org/wg/sidr/>.

[Saucez09]
Saucez, D. and L. Iannone, "How to mitigate the effect of scans on mapping systems", Submitted to the Trilogy Summer School on Future Internet.

## Authors’ Addresses

Damien Saucez
Universite catholique de Louvain
Place St. Barbe 2
Louvain la Neuve
Belgium

Email: damien.saucez@uclouvain.be

Luigi Iannone
TU Berlin - Deutsche Telekom Laboratories AG
Ernst-Reuter Platz 7
Berlin
Germany

Email: luigi@net.t-labs.tu-berlin.de

Olivier Bonaventure
Universite catholique de Louvain
Place St. Barbe 2
Louvain la Neuve
Belgium

Email: olivier.bonaventure@uclouvain.be