Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 13, 2011

D. Saucez
Universite catholique de Louvain
L. Iannone
TU Berlin - Deutsche Telekom Laboratories AG
O. Bonaventure
Universite catholique de Louvain

March 12, 2011

LISP Security Threats
draft-saucez-lisp-security-03.txt

Abstract

This draft analyzes some of the threats against the security of the Locator/Identifier Separation Protocol and proposes a set of recommendations to mitigate some of the identified security risks.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 13, 2011.

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 [I-D.ietf-lisp]. The present document aims at identifying threats in the current LISP specification. We also propose some recommendations on mechanisms that could improve the security of LISP against off-path attackers. This document builds upon [I-D.bagnulo-lisp-threat].

This document is split in two parts. The first discusses the LISP data-plane and the second the LISP control-plane.

The LISP data-plane consists of LISP packet encapsulation, decapsulation, and forwarding and includes the EID-to-RLOC Cache and EID-to-RLOC Database data structures used to perform these operations.

The LISP control-plane consists in the mapping distribution system, which can be one of the mapping distribution systems proposed so far (e.g., [I-D.ietf-lisp], [I-D.ietf-lisp-alt], [I-D.ietf-lisp-ms], [I-D.meyer-lisp-cons], and [I-D.lear-lisp-nerd]), and the Map-Request, Map-Reply, Map-Register messages.

This document does not consider all the possible uses of LISP as discussed in [I-D.ietf-lisp]. In the current version, the document focuses on LISP unicast, including as well LISP Interworking, and briefly considers the ALT mapping system described in [I-D.ietf-lisp-alt]. Later versions of this document will include a deeper analysis of the ALT mapping system, as well as the analysis of the security issues in multicast LISP ([I-D.ietf-lisp-multicast]), interworking between LISP and the legacy IPv4 and IPv6 Internet ([I-D.ietf-lisp-interworking]), and LISP-MS ([I-D.ietf-lisp-ms]).

Furthermore, here we assume a generic IP service and do not discuss the difference from a security viewpoint between using IPv4 or IPv6.

3. Definition of Terms

The present document does not introduce any new term, compared to the main LISP specification. For a complete list of terms please refer to [I-D.ietf-lisp].

4. On-path Attackers

On-path attackers are attackers that are able to capture and modify all the packets exchanged between an ITR and an ETR. To cope with such an attacker, cryptographic techniques such as those used by IPSec are required. We do not consider that LISP has to cope with such attackers.

Mobile IP has also considered time-shifted attacks from on-path attackers. 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 packet flow (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. We do not consider time-shifted attacks in this document.

5. Off-Path Attackers: Reference Environment

Throughout this document we consider the reference environment shown in the figure below. There are two hosts attached to LISP routers: HA and HB. HA is attached to the two LISP xTRs LR1 and LR2, which are attached to two different ISPs. HB is attached to the two LISP xTRs LR3 and LR4. HA and HB are the EIDs of the two hosts. LR1, LR2, LR3, and LR4 are the RLOCs of the xTRs.

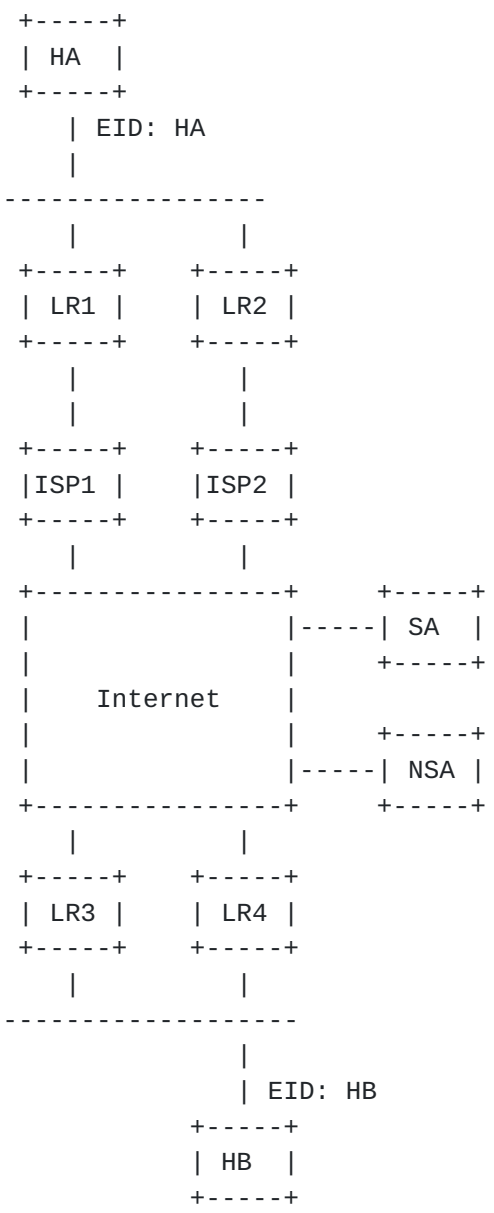

Figure 1: Reference Network

We consider two off-path attackers with different capabilities:

SA is an off-path attacker that is able to send spoofed packets, i.e., packets with a different source IP address than its assigned IP address.

NSA is an off-path attacker that is only able to send packets whose source address is its assigned IP address.

It should be noted that with LISP, packet spoofing is slightly different than in the current Internet. 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, the spoofed address can be in the outer header as well as in the inner header, 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 different kind of attacks.

In our reference environment, both SA and NSA attackers are capable of sending LISP encapsulated data packets and LISP control packets. This means that SA is able to perform both RLOC and EID spoofing while NSA can only perform EID spoofing. They may also send other types of IP packets such as ICMP messages. We assume that both attackers can query the LISP mapping system to obtain the mappings for both HA and HB.

6. Data-Plane Threats

This section discusses threats and attacks related to the LISP data-plane. More precisely, we discuss the operations of encapsulation, decapsulation, and forwarding as well as the content of the EID-to-RLOC Cache and EID-to-RLOC Database as specified in the original LISP document ([I-D.ietf-lisp]).

We start considering the two main data structures of LISP, namely the EID-to-RLOC Database and the EID-to-RLOC Cache. Then, we look at the data plane attacks that can be performed by a spoofing off-path attacker (SA) and discuss how they can be mitigated by the LISP xTRs. In this analysis, we assume that the LR1 and LR2 (resp. LR3 and LR4) xTRs maintain a EID-to-RLOC Cache that contains the required mapping entries to allow HA and HB to exchange packets.

6.1. EID-to-RLOC Database Threats

The EID-to-RLOC Database on each xTR maintains the set of mappings related to the EID-Prefixes that are "behind" the xTR. Where "behind" means that at least one of the xTR's globally-visible IP addresses is a RLOC for those EID-Prefixes.

As described in [I-D.ietf-lisp], the EID-to-RLOC Database content is determined by configuration. This means that the only way to attack this data structure is by gaining privileged access to the xTR. As such, it is out of the scope of LISP to propose any mechanism to protect routers and, hence, it is no further analyzed in this document.

6.2. EID-to-RLOC Cache Threats

A key component of the overall LISP architecture is the EID-to-RLOC Cache. The EID-to-RLOC 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 7) or by corrupting (poisoning) the mappings already present in the cache.

6.2.1. EID-to-RLOC Cache poisoning

The content of the EID-to-RLOC Cache can be poisoned by spoofing LISP encapsulated packets. Example of EID-to-RLOC 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 7.3 or by attacking the control-plane as described in Section 7.

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 7.3 or by attacking the control-plane as described in Section 7.

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 7.3 or by attacking the control-plane as described in Section 7.

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 7. Depending on how the RLOC reachability information is stored on the router, the attack can impact only one mapping or all the mappings that share the same RLOC.

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. It is even possible to block the traffic if all the priorities are set to 255. Corrupting the TE attributes can be achieved by attacking the control-plane as described in Section 7.

Mapping TTL poisoning: The LISP protocol associates a Time-To-Live to each mapping that, once expired, allows to delete a mapping from the EID-to-RLOC 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 EID-to-RLOC 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 6.2.2). Corrupting the TTL can be achieved by attacking the control-plane as described in Section 7. Long TTL can be use in fake mappings to increase an attack duration.

Instance ID poisoning: The LISP protocol allows to use a 24-bit identifier to select the forwarding table to use on the decapsulating ETR to forward the decapsulated packet. By spoofing this attribute the attacker is able to redirect or blackhole inbound traffic. Corrupting the Instance ID attribute can be achieved by attacking the control-plane as described in Section 7.

Map-Version poisoning: The LISP protocol allows to associate a version number to mappings ([I-D.ietf-lisp-map-versioning]). The LISP header can transport source and destination map-versions, describing which version of the mapping have been used to select the source and the destination RLOCs of the LISP encapsulated packet. By spoofing this attribute the attacker is able to trigger Map-Request on the receiving ETR. Corrupting the Map-Version attribute can be achieved either by attacking the control-plane as described in Section 7 or by using spoofed packets as described in Section 6.4.2.

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

6.2.2. EID-to-RLOC Cache overflow

Depending on how the EID-to-RLOC 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 7.3 or by attacking the control-plane as described in Section 7.

Another way to generate a EID-to-RLOC 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.

6.3. Attacks not leveraging on the LISP header

We first consider an attacker that sends packets without exploiting the LISP header, i.e., with the N, L, E, V, and I bits reset ([I-D.ietf-lisp]).

To inject a packet in the HA-HB flow, a spoofing off-path attacker (SA) can send a LISP encapsulated packet whose source is set to LR1 or LR2 and destination LR3 or LR4. The packet will reach HB as if the packet was sent by host HA. This is not different from today's Internet where a spoofing off-path attacker may inject data packets in any flow. Several existing techniques can be used by hosts to prevent such attacks from affecting established flows, e.g., [RFC4301] and [I-D.ietf-tcpm-tcp-security] .

On the other hand, a non-spoofing off-path attacker (NSA) can only send a packet whose source address is set to its assigned IP address. The destination address of the encapsulated packet can be LR3 or LR4. When the LISP ETR that serves HB receives the encapsulated packet, it can consult its EID-to-RLOC Cache and verify that NSA is not a valid source address for LISP encapsulated packets containing a packet sent by HA. This verification is only possible if the ETR already has a valid mapping for HA. Otherwise, and to avoid such data packet injection attacks, the LISP ETR should reject the packet and possibly query the mapping system to obtain a mapping for the encapsulated source EID (HA).

6.4. Attacks leveraging on the LISP header

The latest LISP draft [I-D.ietf-lisp] defines several flags that modify the interpretation of the LISP header in data packets. In this section, we discuss how an off-path attacker could exploit this LISP header.

6.4.1. Attacks using the Locator Status Bits

When the L bit is set to 1, it indicates that the second 32-bits longword of the LISP header contains the Locator Status Bits. In this field, each bit position reflects the status of one of the RLOCs mapped to the source EID found in the encapsulated packet. In particular, a packet with the L bit set and all Locator Status Bits set to zero indicates that none of the locators of the encapsulated source EID are reachable. The reaction of a LISP ETR that receives such a packet is not clearly described in [I-D.ietf-lisp].

A spoofing off-path attacker (SA) can send a data packet with the L bit set to 1, all Locator Status Bits set to zero, a spoofed source RLOC (e.g. LR1), destination LR3, and containing an encapsulated packet whose source is HA. If LR3 blindly trust the Locator Status Bits of the received packet it will set LR1 and LR2 as unreachable, possibly disrupting ongoing communication.

Locator Status Bits can be blindly trusted only in secure environments. In the general unsecured Internet environment, the safest practice for xTRs is to confirm the reachability change through the mapping system. In the above example, LR3 should note that something as changed in the Locator Status Bits and query the mapping system in order to confirm status of the RLOCs of the source EID.

A similar attack could occur by setting only one Locator Status Bit to 1, e.g., the one that corresponds to the source RLOC of the packet.

If a non-spoofing off-path attacker (NSA) sends a data packet with the L bit set to 1 and all Locator Status Bits set to zero, this packet will contain the source address of the attacker. Similarly as in Section 6.3, if the xTR accepts the packet without checking the EID-to-RLOC Cache for a mapping that binds the source EID and the source RLOC of the received packet, then the same observation like for the the spoofing attacker (SA) apply.

Otherwise, if the xTR does make the check through the EID-to-RLOC Cache, it should reject the packet because its source address is not one of the addresses listed as RLOCs for the source EID.

Nevertheless, in this case a Map-Request should be sent, which can be used to perform Denial of Service attacks. Indeed an attacker can frequently change the Locator Status Bits in order to trigger a large amount of Map-Requests. Rate limitation, as described in [I-D.ietf-lisp], does not allow to send high number of such a request, resulting in the attacker saturating the rate with these spoofed packets.

6.4.2. Attacks using the Map-Version bit

The Map-Version bit is used to indicate whether the low-order 24 bits of the first 32 bits word of the LISP header contain an Source and Destination Map-Version. When a LISP ETR receives a LISP encapsulated packet with the Map-Version bit set to 1, the following actions are taken:

- It compares the Destination Map-Version found in the header with the current version of its own mapping, in the EID-to-RLOC Database, for the destination EID found in the encapsulated packet. If the received Destination Map-Version is smaller (i.e., older) than the current version, the ETR should apply the SMR procedure described in [I-D.ietf-lisp] and send a Map-Request with the SMR bit set.

- If a mapping exists in the EID-to-RLOC Cache for the source EID, then it compares the Map-Version of that entry with the Source Map-Version found in the header of the packet. If the stored mapping is older (i.e., the Map-Version is smaller) than the source version of the LISP encapsulated packet, the xTR should send a Map-Request for the source EID.

A spoofing off-path attacker (SA) could use the Map-Version bit to force an ETR to send Map-Request messages. The attacker can retrieve the current source and destination Map-Version for both HA and HB. Based on this information, it can send a spoofed packet with an older Source Map-Version or Destination Map-Version. If the size of the Map-Request message is larger than the size of the smallest LISP-encapsulated packet that could trigger such a message, this could lead to amplification attacks (see Section 7.1). Fortunately, [I-D.ietf-lisp] recommends to rate limit the Map-Request messages that are sent by an xTR. This prevents the amplification attack, but there is a risk of Denial of Service attack if an attacker sends packets with Source and Destination Map-Versions that frequently change. In this case, the ETR could consume all its rate by sending Map-Request messages in response to these spoofed packets.

A non-spoofing off-path attacker (NSA) cannot success in such an attack if the destination xTR rejects the LISP encapsulated packets

that are not sent by one of the RLOCs mapped to the included source EID. If it is not the case, the attacker can be able to perform attacks concerning the Destination Map Version number as for the spoofing off-path attacker (SA).

6.4.3. Attacks using the Nonce-Present and the Echo-Nonce bits

The Nonce-Present and Echo-Nonce bits are used when verifying the reachability of a remote ETR. Assume that LR3 wants to verify that LR1 receives the packets that it sends. LR3 can set the Echo-Nonce and the Nonce-Present bits in LISP data encapsulated packets and include a random nonce in these packets. Upon reception of this packet, LR1 will store the nonce sent by LR3 and echo it when it returns LISP encapsulated data packets to LR3.

A spoofing off-path attacker (SA) could interfere with this reachability test by sending two different types of packets:

1. LISP data encapsulated packets with the Nonce-Present bit set and a random nonce and the appropriate source and destination RLOCs.

2. LISP data encapsulated packets with the Nonce-Present and the Echo-Nonce bits both set and the appropriate source and destination RLOCs. These packets will force the receiving ETR to store the received nonce and echo it in the LISP encapsulated packets that it sends.

The first type of packet should not cause any major problem to ITRs. As the reachability test uses a 24 bits nonce, it is unlikely that an off-path attacker could send a packet that causes an ITR to believe that the ETR it is testing is reachable while in reality it is not reachable.

The second type of packet could be exploited to create a Denial of Service attack against the nonce-based reachability test. Consider a spoofing off-path attacker (SA) that sends a continuous flow of spoofed LISP data encapsulated packets that contain the Nonce-Present and the Echo-Nonce bit and each packet contains a different random nonce. The ETR that receives such packets will continuously change the nonce that it returns to the remote ITR. If the remote ITR starts a nonce-reachability test, this test may fail because the ETR has received a spoofed LISP data encapsulated packet with a different random nonce and never echoes the real nonce. In this case the ITR will consider the ETR not reachable. The success of this test will of course depend on the ratio between the amount of packets sent by the legitimate ITR and the spoofing off-path attacker (SA).

Packets sent by a non-spoofing off-path attacker (NSA) can cause

similar problem if no check is done with the EID-to-RLOC Cache (see Section 6.3 for the EID-to-RLOC Cache check). Otherwise, if the check is performed the packets will be rejected by the ETR that receives them and cannot cause problems.

7. Control Plane Threats

In this section, we discuss the different types of attacks that can occur when an off-path attacker sends control plane packets. We focus on the packets that are sent directly to the ETR and do not analyze the particularities of a LISP mapping system. The ALT mapping system is discussed in Section 10.

7.1. Attacks with Map-Request messages

An off-path attacker could send Map-Request packets to a victim ETR. In theory, a Map-Request packet is only used to solicit an answer and as such it should not lead to security problems. However, the LISP specification [I-D.ietf-lisp] contains several particularities that could be exploited by an off-path attacker.

The first possible exploitation is the P bit. The P bit is used to probe the reachability of remote ETRs in the control plane. In our reference environment, LR3 could probe the reachability of LR1 by sending a Map-Request with the P bit set. LR1 would reply by sending a Map-Reply message with the P bit set and the same nonce as in the Map-Request message.

A spoofing off-path attacker (SA) could use the P bit to force a victim ETR to send a Map-Reply to the spoofed source address of the Map-Request message. As the Map-Reply can be larger than the Map-Request message, there is a risk of amplification attack. Considering only IPv6 addresses, a Map-Request can be as small as 40 bytes, considering one single ITR address and no Mapping Protocol Data. The Map-Reply instead has a size of O(12 + (R * (28 + N * 24))) bytes, where N is the maximum number of RLOCs in a mapping and R the maximum number of records in a Map-Reply. Since up to 255 RLOCs can be associated to an EID-Prefix and 255 records can be stored in a Map-Reply, the maximum size of a Map-Reply is thus above 1 MB showing a size factor of up to 39,193 between the message sent by the attacker and the message sent by the ETR. These numbers are however theoretical values not considering transport layer limitations and it is more likely that the reply will contain only on record with at most a dozen of locators, giving an amplification factor around 8.

Any ISP with a large number of potential RLOCs for a given EID-Prefix

should carefully ponder the best trade-off between the number of RLOCs through which it wants that the EID is reachable and the consequences that an amplification attack can produce.

It should be noted that the maximum rate of Map-Reply messages should apply to all Map-Replies and also be associated to each destination that receives Map-Reply messages. Otherwise, a possible amplification attack could be launched by a spoofing off-path attacker (SA) as follows. Consider an attacker SA and and EID-Prefix p/P and a victim ITR. To amplify a Denial of Service attack against the victim ITR, SA could send spoofed Map-Request messages whose source EID addresses are all the addresses inside p/P and source RLOC address is the victim ITR. Upon reception of these Map-Request messages, the ETR would send large Map-Reply messages for each of the addresses inside p/P back to the victim ITR.

If a non-spoofing off-path attacker (NSA) sends a Map-Request with the P bit set, it will receive a Map-Reply with the P bit set. This does not raise security issues besides the usual risk of overloading a victim ETR by sending too many Map-Request messages.

The Map-Request message may also contain the SMR bit. Upon reception of a Map-Request message with the SMR bit, an ETR must return to the source of the Map-Request message a Map-Request message to retrieve the corresponding mapping. This raises similar problems as the P bit discussed above except that as the Map-Request messages are smaller than Map-Reply messages, the risk of amplification attacks is reduced. This is not true anymore if the ETR append to the Map-Request messages its own Map-Records. This mechanism is meant to reduce the delay in mapping distribution since mapping information is provided in the Map-Request message.

Furthermore, appending Map-Records to Map-Request messages represents a major security risk since an off-path attacker could generate a (spoofed or not) Map-Request message and include in the Map-Reply portion of the message mapping for EID prefixes that it does not serve. This could lead to various types of redirection and denial of service attacks. An xTR should not process the Map-Records information that it receives in a Map-Request message.

7.2. Attacks with Map-Reply messages

In this section we analyze the attacks that could occur when an off-path attacker sends directly Map-Reply messages to ETRs without using one of the proposed LISP mapping systems.

There are two different types of Map-Reply messages:

Positive Map-Reply: This messages contain a Map-Record binding an EID-Prefix to one or more RLOCs.

Negative Map-Reply: This messages contain a Map-Record for an EID-Prefix with an empty locator-set and specifying an action, which may be either Drop, Natively forward, or Send Map-Request.

Positive Map-Reply messages are used to map EID-Prefixes onto RLOCs. Negative Map-Reply messages are used to support PTR and interconnect the LISP Internet with the legacy Internet.

Most of the security of the Map-Reply messages depend on the 64 bits nonce that is included in a Map-Request and returned in the Map-Reply. An ETR must never accept a Map-Request message whose nonce does not match one of the pending Map-Request messages. If an ETR does not accept Map-Reply messages with an invalid nonce, the risk of attack is very small given the size of the nonce (64 bits).

Note, however, that the nonce only confirms that the Map-Reply was sent by the ETR that received the Map-Request. It does not validate the content of the Map-Reply message.

7.3. Gleaning Attacks

A third type of attack involves the gleaning mechanism proposed in [I-D.ietf-lisp] and discussed in [Saucez09]. In order to reduce the time required to obtain a mapping, [I-D.ietf-lisp] allows an ITR to learn a mapping from the LISP data encapsulated packets and the Map-Request packets that it receives. LISP data encapsulated packet contains a source RLOC, destination RLOC, source EID and destination EID. When a ITR receives a data encapsulated packet coming from a source EID for which it does not already know a mapping, it may insert the mapping between the source RLOC and the source EID in its EID-to-RLOC Cache. Gleaning can also be used when an ITR receives a Map-Request as the Map-Request also contains a source EID address and a source RLOC. Once a gleaned entry has been added to the cache, the LISP ITR sends a Map-Request to retrieve the mapping for the gleaned EID from the mapping system. [I-D.ietf-lisp] recommends to store the gleaned entries for only a few seconds.

The first risk of gleaning is the ability to temporarily hijack an identity. Consider an off-path attacker that wants to temporarily hijack host HA's identity and send packets to host HB with host HA's identity. If the xTRs that serve host HB do not store a mapping for host HA, a non-spoofing off-path attacker (NSA) could send a LISP encapsulated data packet to LR3 or LR4. The ETR will store the gleaned entry and use it to return the packets sent by host HB to the

attacker. In parallel, the ETR will send a Map-Request to retrieve the mapping for HA. During a few seconds or until the reception of the Map-Reply, host HB will exchange packets with the attacker that has hijacked HA's identity. Note that the attacker could in parallel send lots of Map-Requests or lots of LISP data encapsulated packets with random sources to force the xTR that is responsible for host HA to send lots of Map-Request messages in order to force it to exceed its rate limit for control plane messages. This could further delay the arrival of the Map-Reply message on the requesting ETR.

Gleaning also introduces the possibility of a man-in-the-middle attack. Consider an off-path attacker that knows that hosts HA and HB that reside in different sites will exchange information at time t. An off-path attacker could use this knowledge to launch a man-in-the-middle attack if the xTRs that serve the two hosts do not have mapping for the other EID. For this, the attacker sends to LR1 (resp. LR3) a LISP data encapsulated packet whose source RLOC is its IP address and contains an IP packet whose source is set to HB (resp. HA). The attacker chooses a packet that will not trigger an answer, for example the last part of a fragmented packet. Upon reception of these packets, LR1 and LR3 install gleaned entries that point to the attacker. As explained above, the attacker could, at the same time, send lots of packets to LR1 and LR3 to force them to exhaust their control plane rate limit. This will extend the duration of the gleaned entry. If host HA establishes a flow with host HB at that time, the packets that they exchange will first pass through the attacker.

In both cases, the attack only lasts for a few seconds (unless the attacker is able to exhaust the rate limitation). However it should be noted that today a large amount of packets may be exchanged during even a small fraction of time.

8. Threats concerning Interworking

[I-D.ietf-lisp-interworking] defines two network elements to allow LISP and non-LISP sites to communicate, namely the Proxy-ITR and the Proxy-ETR. The Proxy-ITR encapsulates traffic from non-LISP sites in order to forward it toward LISP sites, while the Proxy-ETR decapsulates traffic arriving from LISP sites in order to forward it toward non-LISP sites. For these elements some of the attack based on the LISP specific header are not possible, for the simple reason that some of the fields cannot be used due to the unidirectional nature of the traffic.

The Proxy-ITR has functionalities similar to the ITR, however, its main purpose is to encapsulate packets arriving from the DFZ in order

to reach LISP sites. This means that it is no bound to any particular EID-Prefix, hence no mapping exists and no mapping can be configured in the EID-to-RLOC Database. This means that the Proxy-ITR element itself is not able, to check whether or not the arriving traffic has the right to be encapsulated or not. To limit such an issue it is recommended to use the current practice based on firewalls and ACLs on the machine running the Proxy-ITR service. On the other side, the Proxy-ITR is meant to encapsulate only packets that are destined to one of the LISP sites it is serving. This is the case for instance for a service provider selling Proxy-ITR services. For this purpose a static EID-to-RLOC Cache can be configured in order to encapsulate only valid packets. In case of a cache-miss no Map-Request needs to be sent and the packet can be silently dropped.

The Proxy-ETR has functionalities similar to the ETR, however, its main purpose is to inject un-encapsulated packet in the DFZ in order to reach non-LISP-Sites. This means that since there is no specific EID-Prefix downstream, it has no EID-to-RLOC Database that can be used to check whether or not the destination EID is part of its domain. In order to avoid for the Proxy-ETR to be used as relay in a DoS attack it is preferable to configure the EID-to-RLOC Cache with static entries used to check if an encapsulated packet coming from a specific RLOC and having a specific source EID is actually allowed to transit through the Proxy-ETR. This is also important for services provider selling Proxy-ETR service to actually process only packets arriving from its customers. However, in case of cache-miss no Map-Request needs to be sent, rather the packet can be silently dropped since it is not originating from a valid site. The same drop policy should be used for packets with an invalid source RLOC or a valid source RLOC but an invalid EID.

9. Threats with Malicious xTRs

In this section, we discuss the threats that could be caused by malicious xTRs. We consider the reference environment below where EL1 is a malicious or compromised xTR. This malicious xTR serves a set of hosts that includes HC. The other xTR and hosts in this network play the same role as in the reference environment described in Section 5.

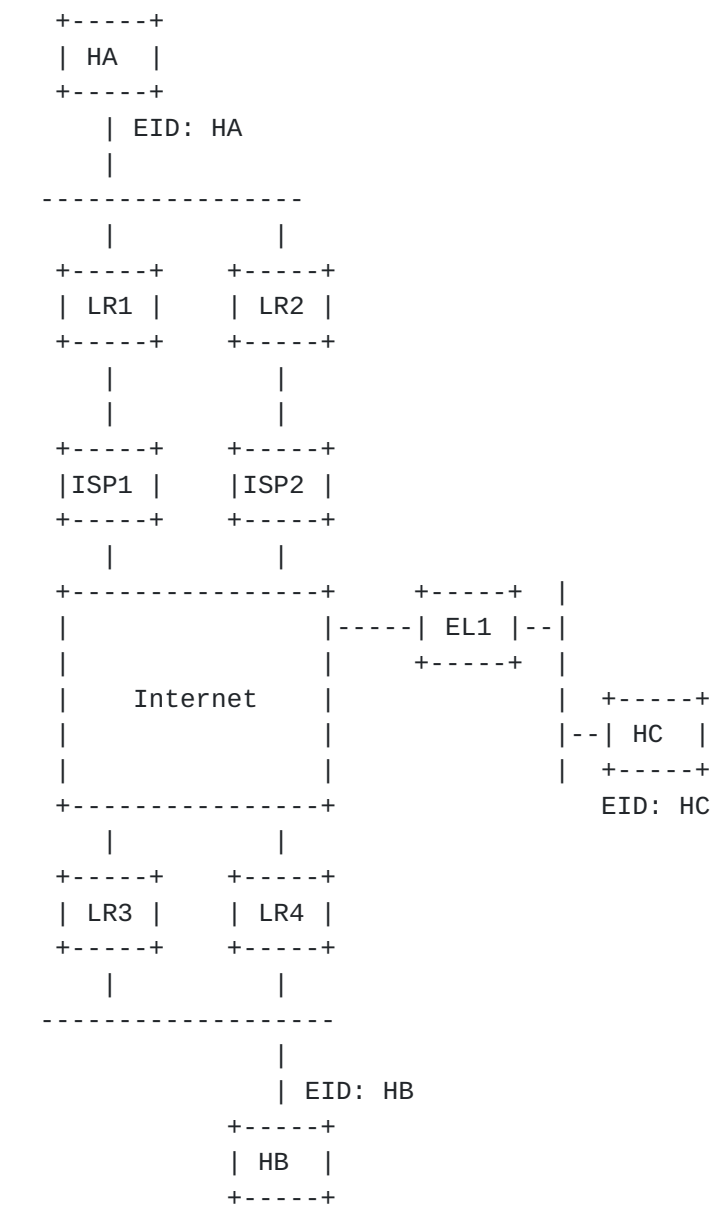

Figure 2: Malicious xTRs' Reference Environment

Malicious xTRs are probably the most serious threat to the LISP control plane from a security viewpoint. To understand the problem, let us consider the following scenario. Host HC and HB exchange packets with host HA. As all these hosts reside in LISP sites, LR1 and LR2 store mappings for HB and HC. Thus, these xTRs may need to exchange LISP control plane packets with EL1, e.g., to perform reachability tests or to refresh expired mappings (e.g., if HC's mapping has a small TTL).

A first threat against the LISP control plane is when EL1 replies to a legitimate Map-Request message sent by LR1 or LR2 with a Map-Reply

message that contains an EID-Prefix that is larger than the prefix owned by the site attached to EL1. This could allow EL1 to attract packets destined to other EIDs than the EIDs that are attached to EL1.

Another possible attack is a Denial of Service attack by sending a Negative Map-Reply message for a coarser prefix without any locator and with the Drop action. Such a Negative Map-Reply indicates that the ETR that receives it should discard all packets. The current LISP specification briefly discusses this problem [I-D.ietf-lisp], but the proposed solutions does not solve the problem.

Another concern with malicious xTRs is the possibility of Denial of Service attacks. A first attack is the flooding attack that was described in [I-D.bagnulo-lisp-threat]. This attack allows a malicious xTR to redirect traffic to a victim. The malicious xTR first defines a mapping for HC with two RLOCs: its own RLOC (EL1) and the RLOC of the victim (e.g., LR3). The victim's RLOC is set as unreachable in the mapping. HC starts a large download from host HA. Once the download starts, the malicious xTR updates its Locator Status Bits, changes the mapping's version number or sets the SMR bit such that LR1 updates its EID-to-RLOC Cache to send all packets destined to HC to the victim's RLOC. Instead of downloading from HA, the attacker could also send packets that trigger a response (e.g., ICMP, TCP SYN, DNS request, ...) to HA. HA would then send its response and its xTR would forward it to the victim's RLOC.

An important point to note about this flooding attack is that it reveals a potential problem in the LISP architecture. A LISP ITR relies on the received mapping and possible reachability information to select the RLOC of the ETR that it uses to reach a given EID or block of EIDs. However, if the ITR made a mistake, e.g., due to configuration, implementation or other types of errors and has chosen a RLOC that does not serve the destination EID, there is no easy way for the LISP ETR to inform the ITR of its mistake. A possible solution could be to force a ETR to perform a reachability test with the selected ITR as soon as it selects it. This will be analyzed in the next version of this document.

10. Security of the ALT Mapping System

One of the assumptions in [I-D.ietf-lisp] is that the mapping system is more secure than sending Map-Request and Map-Reply messages directly. We analyze this assumption in this section by analyzing the security of the ALT mapping system.

The ALT mapping system is basically a manually configured overlay of

GRE tunnels between ALT routers. BGP sessions are established between ALT routers that are connected through such a tunnel. An ALT router advertises the EID prefixes that it serves over its BGP sessions with neighboring ALT routers and the EID-Prefixes that it has learned from neighboring ALT routers.

The ALT mapping system is in fact a discovery system that allows any ALT router to discover the ALT router that is responsible for a given EID-Prefix. To obtain a mapping from the ALT system, an ITR sends a packet containing a Map-Request on the overlay. This Map-Request is sent inside a packet whose destination is the requested EID. The Map-Request is routed on the overlay until it reaches the ALT router that advertised initially the prefix that contains the requested EID. This ALT router then replies directly by sending a Map-Reply to the RLOC of the requesting ITR.

The security of the ALT mapping system depends on many factors, including:

- The security of the intermediate ALT routers.
- The validity of the BGP advertisements sent on the ALT overlay.

Unfortunately, experience with BGP on the global Internet has shown that BGP is subject to various types of misconfiguration problems and security attacks. The SIDR working group is developing a more secure inter-domain routing architecture to solve this problem ([I-D.ietf-sidr-arch]).

The security of the intermediate ALT routers is another concern. A malicious intermediate ALT router could manipulate the received BGP advertisements and also answer to received Map-Requests without forwarding them to their final destination on the overlay. This could lead to various types of redirection attacks. Note that in contrast with a regular IP router that could also manipulate in transit packets, when a malicious or compromised ALT router replies to a Map-Request, it can redirect legitimate traffic for a long period of time by sending an invalid Map-Reply message. Thus, the impact of a malicious ALT router could be much more severe than a malicious router in today's Internet.

11. Suggested Recommendations

To mitigate the impact of attacks against LISP, the following recommendations should be followed.

First, the use of some form of filtering can help in avoid or at

least mitigate some types of attacks.

- 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 EID-to-RLOC Cache and has been obtained through the mapping system (not gleaned).

- 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 EID-to-RLOC Cache (no Data-Probing).

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 EID-to-RLOC Cache.

While the gleaning mechanism allows to start encapsulating packets to a certain EID in parallel with the Map-Request to obtain a mapping when a new flow is established, it creates important security risks since it allows attackers to perform identity hijacks. Although the duration of these identity hijacks is limited (except the case of rate limitation exhaustion), their impact can be severe. A first option would be to disable gleaning until the security concerns are solved. A second option would be to strictly limit the number of packets that can be forwarded via a gleaned entry. Overall the benefits of gleaning, i.e., avoiding the loss of the first packet of a flow, seems very small compared to the associated security risks. Furthermore, measurements performed in data centers show that today's Internet often operate with packet loss ratio of 1 or 2 percentage ([Chu]). These packet loss ratio are probably already orders of magnitude larger than the improvement provided by the gleaning mechanism.

With the increasing deployment of spoofing prevention techniques such as [RFC3704] or SAVI [SAVI], it can be expected that attackers will become less capable of sending packets with a spoofed source address. To prevent packet injection attacks from non-spoofing attackers (NSA), ETRs should always verify that the source RLOC of each received LISP data encapsulated packet corresponds to one of the RLOCs listed in the mappings for the source EID found in the inner packet. An alternative could be to use existing IPSec techniques [RFC4301]and when necessary including perhaps [RFC5386] to establish an authenticated tunnel between the ITR and the ETR.

[I-D.ietf-lisp] recommends to rate limit the control messages that

are sent by a xTR. This limit is important to deal with denial of service attacks. However, a strict limit, e.g., implemented with a token bucket, on all the Map-Request and Map-Reply messages sent by a xTR is not sufficient. A xTR should distinguish between different types of control plane packets:

1. The Map-Request messages that it sends to refresh expired mapping information.

2. The Map-Request messages that it sends to obtain mapping information because one of the served hosts tried to contact an external EID.

3. The Map-Request messages that it sends as reachability probes.

4. The Map-Reply messages that it sends as response to reachability probes.

5. The Map-Request messages that it sends to support gleaning.

These control plane messages are used for different purposes. Fixing a global rate limit for all control plane messages increases the risk of Denial of Service attacks if a single type of control plane message can exceed the configured limit. This risk could be mitigated by either specifying a rate for each of the five types of control plane messages. Another option could be to define a maximum rate for all control plane messages, and prioritize the control plane messages according to the list above (with the highest priority for message type 1).

In [I-D.ietf-lisp], there is no mechanism that allows a xTR to verify the validity of the content a Map-Reply message that it receives. Besides the attacks discussed earlier in the document, a time-shifted attack where an attacker is able to modify the content of a Map-Reply message but then needs to move off-path could also create redirection attacks. The nonce only allows a xTR to verify that a Map-Reply responds to a previously sent Map-Request message. The LISP Working Group should explore solutions that allow to verify the validity and integrity of bindings between EID-Prefixes and their RLOCS (e.g., [I-D.saucez-lisp-mapping-security] and [I-D.maino-lisp-sec]). Having such kind of mechanism would allow ITRs to ignore non-verified mappings, thus increasing security.

LISP Working Group should consider developing secure mechanisms to allow an ETR to indicate to an ITR that it does not serve a particular EID or block of EIDs in order to mitigate the flooding attacks.

Finally, there is also the risk of Denial of Service attack against the EID-to-RLOC Cache. We have discussed these attacks when considering external attackers with, e.g., the gleaning mechanism and in Section 6.2. If an ITR has a limited EID-to-RLOC Cache, a malicious or compromised host residing in the site that it serves could generate packets to random destinations to force the ITR to issue a large number of Map-Requests whose answers could fill its cache. Faced with such misbehaving hosts, LISP ITR should be able to limit the percent of Map-Requests that it sends for a given source EID.

12. Document Status and Plans

In this document, we have analyzed some of the security threats that affect the Locator/Identifier Separation Protocol (LISP). We have focused our analysis on unicast traffic and considered both the LISP data and control planes, and provided some recommendations to improve the security of LISP.

Revisions of this document will document the security threats of other parts of the LISP architecture, including but not limited to:

- Instance ID attribute.
- LISP Multicast.
- LISP Map-Server.

13. IANA Considerations

This document makes no request to IANA.

14. Security Considerations

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

15. Acknowledgments

The flooding attack and the reference environment were first described in Marcelo Bagnulo's draft [I-D.bagnulo-lisp-threat].

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

16. References

16.1. Normative References

[I-D.ietf-lisp]
Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol (LISP)", draft-ietf-lisp-10 (work in progress), March 2011.

[I-D.ietf-lisp-alt]
Fuller, V., Farinacci, D., Meyer, D., and D. Lewis, "LISP Alternative Topology (LISP+ALT)", draft-ietf-lisp-alt-06 (work in progress), March 2011.

[I-D.ietf-lisp-interworking]
Lewis, D., Meyer, D., Farinacci, D., and V. Fuller, "Interworking LISP with IPv4 and IPv6", draft-ietf-lisp-interworking-02 (work in progress), March 2011.

[I-D.ietf-lisp-map-versioning]
Iannone, L., Saucez, D., and O. Bonaventure, "LISP Map-Versioning", draft-ietf-lisp-map-versioning-01 (work in progress), March 2011.

[I-D.ietf-lisp-ms]
Fuller, V. and D. Farinacci, "LISP Map Server", draft-ietf-lisp-ms-07 (work in progress), March 2011.

[I-D.ietf-lisp-multicast]
Farinacci, D., Meyer, D., Zwiebel, J., and S. Venaas, "LISP for Multicast Environments", draft-ietf-lisp-multicast-04 (work in progress), October 2010.

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

16.2. Informative References

[Chu] Jerry Chu, H., "Tuning TCP Parameters for the 21st Century", 75th IETF, Stockholm, July 2009, <http://tools.ietf.org/wg/savi/>.

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

[I-D.ietf-sidr-arch]
Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", draft-ietf-sidr-arch-12 (work in progress), February 2011.

[I-D.ietf-tcpm-tcp-security]
Gont, F., "Security Assessment of the Transmission Control Protocol (TCP)", draft-ietf-tcpm-tcp-security-02 (work in progress), January 2011.

[I-D.lear-lisp-nerd]
Lear, E., "NERD: A Not-so-novel EID to RLOC Database", draft-lear-lisp-nerd-08 (work in progress), March 2010.

[I-D.maino-lisp-sec]
Maino, F., Ermagan, V., Cabellos-Aparicio, A., Saucez, D., and O. Bonaventure, "LISP-Security (LISP-SEC)", draft-maino-lisp-sec-00 (work in progress), March 2011.

[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.

[I-D.saucez-lisp-mapping-security]
Saucez, D. and O. Bonaventure, "Securing LISP Mapping replies", draft-saucez-lisp-mapping-security-00 (work in progress), February 2011.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5386] Williams, N. and M. Richardson, "Better-Than-Nothing Security: An Unauthenticated Mode of IPsec", RFC 5386, November 2008.

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

[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