Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 24, 2011

D. Saucez
O. Bonaventure
Universite catholique de Louvain
February 20, 2011

Securing LISP Mapping replies
draft-saucez-lisp-mapping-security-00

Abstract

The security of the mappings is crucial for the success of the Locator/Identifier Separation Protocol (LISP). This draft discusses two options to allow LISP xTR to verify the authenticity of LISP Map-Replies.

Table of Contents

1. Introduction

The Locator/Identifier Separation Protocol (LISP) is currently being developed with the LISP IETF working group [I-D.ietf-lisp]. LISP can be conceptually divided in two different parts :

- LISP data plane that defines the format and the processing of LISP encapsulated packets on xTRs
- LISP control plane that defines how an ITR obtains mapping information about a destination EID and manages this information.

The LISP control plane plays a key role from a security viewpoint in the entire operation of LISP. LISP xTRs exchange mapping information by using Map-Requests and Map-Replies. It is important to note that the LISP control plane messages are used for three different purposes by ITRs and ETRs:

- When a LISP ITR does not know any mapping information for an EID, it sends a LISP Map-Request through the LISP Mapping system. The LISP Mapping system will ensure that the LISP Map-Request will reach a LISP Mapping Server or a LISP ETR that is authoritative for the requested EID. A LISP ETR will then send a LISP Map-Reply directly to the originating LISP ITR.
- When a mapping information times out on a LISP ITR, the ITR will need to refresh the mapping by either sending a LISP Map-Request through the LISP Mapping System or directly to one of the LISP ETR that is responsible for the expired mapping. One of the authoritative LISP ETR will then send a LISP Map-Reply directly to the originating LISP ITR.
- A LISP ITR may send a LISP Map-Request directly to a LISP ETR to verify its reachability. The ETR will confirm its reachability by sending a LISP Map-Reply back.

The security of the LISP control plane is crucial for the security of LISP. A detailed discussion on the security of LISP may be found in [I-D.saucez-lisp-security]. The current LISP specifications do not provide a secure LISP Mapping System. The ALT [I-D.ietf-lisp-alt] Mapping system relies on BGP sessions established manually over tunnels between LISP xTRs and LISP Mapping Servers. ALT assumes that such a mapping system will be secure since it is operated by trusted operators. Unfortunately, the experience with BGP on the global Internet has shown that this is not a valid assumption and that additional techniques are required to secure a routing system that relies on BGP.

This document is organized as follows. In Section 2 we present the different levels of security that can be provided and analyze their respective advantages and drawbacks. In Section 4 we discuss several families of solutions that can be designed to improve the security of the LISP control plane.

2. Mapping security levels

The level security of a mapping is determined by the level of confidence that a LISP xTR can have on information obtained through it.

By using nonce mechanism as described in the LISP specifications, a LISP ITR can be confident that a Map-Reply it receives has been sent by the LISP ETR that it queried. This is relevant when an ITR sends a Map-Request directly to a LISP ETR that it already knows. However, when a LISP ITR sends a Map-Request through the LISP mapping system, the Map-Reply may come from any LISP ETR and that fact that it contains the same nonce as in the LISP Map-Request only proves that it was generated in response to a specific Map-Request. Indeed, the 64-bits nonce that must be returned by the ETR mitigates the risk of injection attacks where an attacker inject Map-Replies containing invalid information. Unfortunately, if the attacker is on path, it may intercept the Map-Request and extract its nonce. It can then generate a Map-Reply that looks authentic for the ITR as the nonce in the reply is valid. The nonce thus provides only a simple way of authenticating the Map-Replies when man-in-the middle attacks are not possible.

If messages can be tampered, or if man-in-the middle attacks are possible, or if the mapping system may be abused to deliver to a hostile ETR a Map-Request sent by an ITR, we need a better security than the nonce.

3. Requirements to secure Mapping information

LISP Map-Reply messages contain several types of mapping information. In this section, we evaluate the security risks if an attacker is able to inject invalid mapping information. We consider that the LISP nonce protects against injection of Map-Reply messages by an off-path attacker and discuss two types of attackers:

An attacker that temporarily resides on the path between an ITR and an ETR and is able to perform a man-in-the-middle attack by modifying Map-Reply messages exchanged between these xTRs. We call this attacker the on-path attacker in this document.

A malicious xTR or LISP-MS that receives legitimate Map-Request messages from ITRs but returns crafted Map-Reply messages. We call this attacker the malicious xTR in this document.

The mapping information and their associated security risk is presented below:

- EID prefix and mask length. By changing the EID prefix in a Map-Reply message, an on-path attacker could cause denial of service attacks of blackhole traffic by placing in the Map-Reply message a less specific EID prefix than in the original Map-Reply. A malicious xTR could also return a less specific prefix and blackhole traffic.

- Locator. The locators are probably the most important information in the LISP Map-Reply messages since they indicate where encapsulated packets should be sent to reach a given EID prefix. By changing locators, an on-path attacker could redirect traffic to another LISP ETR where it can perform man-in-the-middle attacks on encapsulated packets more easily. By injecting incorrect RLOCs, a malicious xTR could also redirect encapsulated traffic to a LISP ETR where it can easily perform a man-in-the-middle attack.

- Priority and Multicast Priority. If an attacker is able to change the priority associated to a locator in a mapping, it could force an ITR to send encapuslated packets over another path than the intended path. It can also make any RLOC unused by setting it a 255 priority.

- Weight and Multicast Weight. This field is used to influence how load balancing should be performed when several locators have the same priority. By changing weight, an attacker could move encapsulated packets over different paths.

- Record TTL. By lowering the record TTL, an attacker could force an ITR to send more frequently Map-Request messages. By increasing the record TTL, an attacker could ensure that a fake mapping information is used for a longer time by its victim. A temporarily on-path attacker could use a long record to ensure that a malicious mapping remains in the victim ITR EID-to-RLOC cache for a long period of time.

- Version. By changing the Version of a mapping, an attacker could trigger a loop of mapping updates at the ITR. Indeed, if the version is invalid, when the ITR receives a packet from the EID it received the mapping for, it will send a Map-Request as the version does not correspond. If the attacker can control the version of the Map-Reply, this scheme can be repeated

indefinitely.

- Reachability. If an attacker is able to change the reachability bit associated to a locator, it could force a LISP ITR to test the reachability of this locator.

Based on the analysis above, the most critical information in the mapping placed in LISP Map-Reply messages are the EID prefixes and the locators. From a security viewpoint, it is important for a LISP ITR to be able to verify the validity of the link between an EID prefix and a set of locators.

4. Mapping Authentication Mechanisms

To authenticate the mappings, several techniques can be used. Authenticating mapping information is similar to validate DNS responses and also related to the validation of BGP prefixes in the global interdomain routing system. In this section, we discuss the applicability of two techniques that have been designed to secure interdomain routing to secure LISP mappings.

4.1. Mapping Authenticity Base

The first technique that was developed to verify the authenticity of BGP announcements are the prefix allocation databases maintained by the Regional Internet Registries. Each RIR maintains a database, typically in RPSL format, that contains the list of all the prefixes that have been allocated to a given AS. An AS can use this information to verify the received BGP advertisements. Some operators use filters that are automatically derived from the RIR databases and installed on their BGP import filters. Experience shows that this method works reasonably well in some regions and that it is able to prevent misconfiguration problems. However, it can be difficult to maintain the RIR databases up-to-date.

The allocation of EID prefixes by RIRs has not yet been precisely discussed within the LISP working group, but a possible approach could be as follows. Sites obtain EID prefixes from a RIR or a LIR and register on the RIR database the locators of the ETR that serve each allocated EID prefix. The list of locators that are associated to an EID prefix is only the list of the potential locators. The RIR database, unlike the NERD mapping system would not contain detailed information about the mapping such as priorities or weights. This information may change with time and should be obtained by querying the mapping system.

When an ITR needs a mapping for an EID prefix that it does not know,

it queries the mapping system as usual and receives an unauthenticated Map-Reply. Two techniques could be developed to allow the ITR to verify the validity of the received Map-Reply based on the information stored in the RIR databases. A first option is that the network administrator that is responsible for an ITR downloads regularly the RIR database and derives filters for all the valid pairs of EID prefix - RLOC. These filters are regularly pushed on the LISP ITRs and are used to verify each received LISP Map-Reply.

A second solution is to allow each LISP ITR to directly query the RIR database by using either an existing protocol such as whois or a new protocol to be developed. This allows the ITR to verify in realtime the LISP Map-Replies that it receives, but imposes a possibly high load on the RIR databases.

The advantage of using the RIR databases is that there is already a lot of operational experience with them. However, the load on the RIR databases can be high. Furthermore, updating the RIR databases might be difficult for LISP ETRs that use dynamic routing locators, e.g. RLOCs assigned by DHCP.

4.2. Signed Mappings

The Mapping Authenticity Base approach has the advantage of keeping the Map-Reply processing light at the ITR and the ETR. Unfortunately, running the authenticity base could cause administrative and cost overhead and the system has still some security weaknesses.

Instead of using a separated infrastructure to authenticate the mappings, we can embed the authentication scheme directly in the mapping messages. With this approach, each mapping message is signed.

To reduce the processing at the ETR, we will consider that only the Map-Replies are signed. We still have to determine if it is required to authenticate the Map-Requests.

Depending on the security level that has to be reached, different part of the mapping have to be signed.

Adding a field in the Map-Reply that is the signature of the hash of the ETR address and the nonce is not sufficient as it does not protect against tempering, it only confirms that the Map-Reply has been initially generated by the appropriated ETR the content may have been tempered.

For a higher level of security, a certificate has to be used, the certificate gives the EID prefix and the proof that the EID prefix

belongs to the ETR (e.g., the certificate is signed by a well-known

EID registry). A field is added to the Map-Reply and contains the signature of the hash of the ETR address, the nonce and the EID prefix. This signature prove that the EID prefix belongs to the ETR and that the correct ETR has been queried. The set of RLOCs and the mapping attributes may still have been tempered.

To also prove that the locators are valid and thus avoid divert traffic attacks, the same principle as before can be followed but the certificate adds the list of valid RLOCs for the EID prefix. The signature covers the ETR address, the nonce, the EID prefix and the RLOCs.

To reach an ultimate security level, the technique from above can be used but it has to be applied to all the mapping fields, the ETR address and the nonce.

When signing the entire message improves the security by virtually prohibiting any modification of the message, it can cause an important overhead at the ETR and the signature cannot be pre-computed (i.e., the nonce makes the message changing every time. On the contrary, signing only some parts of the message could allow one to pre-compute the signature and thus make the generation of a Map-Reply not more complex than the generation of a Map-Reply without a signature.

An attack can at most replay a mapping that has been valid in the past. The injection of old mappings by attackers can be mitigate if the certificate associated to the mapping are limited in time. This expiration date has to be set accordingly to the security needs of the site generating the mapping.

When the signature does not cover the all message, pre-computation can be used to compute the signature. In this case, the signature is computed when the mapping is installed in the local mapping database.

The pre-computation of the signature allows to avoid the cost of computing the signature at each request on the ETRs and thus make the ETR insensible to DDoS attacks that could target an ETR by asking it to perform time consuming cryptography operations.

The validation of the signature at the ITR is always present but its impact is limited compared to doing signatures at the ETR on the fly. In addition, if the ITR is overloaded, it could decide to postpone the authenticity check but use the mapping anyway.

We can also propose intermediate security level where only some part of the mapping are authenticated. We suggest to cover the TTL, the

EID prefix and the list of [locator, priority, weight] tuples. We removed the reachability information from the authentication as it is more volatile than the mappings and signature computation would be triggered after every reachability change. At a first glance, not signing the reachability seems to be a mistake because an attacker could set all the reachability bit of each RLOC to zero and thus block the traffic. However, as for locator status bits, we are considering this information as a hint, a reachability change has to be validated first with a reachability algorithm before effectively considering the reachability change. Indeed, the reachability is a local consideration.

5. Security Considerations

This document is entirely devoted to the security

6. Conclusion

TO DO

7. Acknowledgments

The authors would like to gratefully acknowledge Luigi Iannone for his insights.

8. Informative References

[I-D.ietf-lisp]
Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol (LISP)", draft-ietf-lisp-09 (work in progress), October 2010.

[I-D.ietf-lisp-alt]
Fuller, V., Farinacci, D., Meyer, D., and D. Lewis, "LISP Alternative Topology (LISP+ALT)", draft-ietf-lisp-alt-05 (work in progress), October 2010.

[I-D.saucez-lisp-security]
Saucez, D., Iannone, L., and O. Bonaventure, "LISP Security Threats", draft-saucez-lisp-security-01 (work in progress), July 2010.

Authors' Addresses

Damien Saucez
Universite catholique de Louvain
Place St. Barbe 2
Louvain-la-Neuve, B-1348
Belgium

Email: damien.saucez@uclouvain.be
URI: http://inl.info.ucl.ac.be

Olivier Bonaventure
Universite catholique de Louvain
Place St. Barbe 2
Louvain-la-Neuve, B-1348
Belgium

Email: olivier.bonaventure@uclouvain.be
URI: http://inl.info.ucl.ac.be