

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 9, 2018

D. von Hugo
Deutsche Telekom
B. Sarikaya
Denpel Informatique
T. Herbert
Quantonium
L. Iannone
Telecom ParisTech
June 7, 2018

Gap and Solution Space Analysis for End to End Privacy Enabled Mapping
System
draft-xyzy-atick-gaps-01.txt

Abstract

This document presents a gap and solution analysis for end-to-end privacy enabled mapping systems. Each of the identifier locator separation system has its own approach to mapping identifiers to the locators. We analyse all these approaches and identify the gaps in each of them and do a solution space analysis in an attempt to identify a mapping system that can be end to end privacy enabled.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on December 9, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

Internet-Draft

Atick Gap Analysis

June 2018

(<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Conventions and Terminology	3
3.	Gap and Solution Space Analysis	3
3.1.	ILA	3
3.2.	LISP	4
4.	General Recommendations	5
4.1.	Security In the Data Path	5
5.	IANA Considerations	6
6.	Security Considerations	6
7.	Acknowledgements	6
8.	References	6
8.1.	Normative References	6
8.2.	Informative References	7
	Authors' Addresses	8

[1.](#) Introduction

Identifier Locator Systems like ILA [[I-D.herbert-intarea-ila](#)], LISP [[I-D.ietf-lisp-rfc6830bis](#)] [[I-D.ietf-lisp-rfc6833bis](#)] and others are proposed as alternative approaches to enabling direct routing in the upcoming converged communication networks such as 5G core network (5GC) rather than using tunneling with GTP-U, GRE, (P)MIPv6 or similar ones. In addition to increasing packet overhead due to encapsulation that may cause fragmentation and all related issues typical disadvantages of (especially static end-to-end) tunneling comprise inflexibility to properly react to dynamic changes of end points and potential on-path anchors. Added complexity in case of multicast traffic and increased signaling for tunnel management are further drawbacks. Tunnels may introduce vulnerabilities or add to the potential for receiver overload and thus DOS attacks [[draft-ietf-intarea-tunnels-08](#)]. Finally without other measures such as deep packet inspection optimization of paths according to network resources and application needs becomes complex.

With the Id-Loc systems a mapping system needs to be established so that 5GC nodes or functions can access the identifier and locator values of the destination given the source identifier and locator values to enable them to route the packet towards the destination.

For mapping systems there will be a trade-off between scalability and rapid processing versus privacy and security of data.

A public distributed database such as the DNS is used by end hosts for host name (or FQDN) to identifier mapping usually to start the communication. DNS can be used to publicly access identifiers. However, using DNS for locator access brings the issue that any node in the internet can query and track the location of the roaming UEs in 5G network which is not desirable. A separate database called a mapping system needs to be used for identifier to locator mapping. Such a mapping system need not be public in order to avoid that any node can write new mapping pairs or ID-Loc bindings in such a database.

[2.](#) Conventions and Terminology

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 [RFC 2119](#) [[RFC2119](#)].

See the definitions in [[I-D.xyz-atick-ps](#)].

[3.](#) Gap and Solution Space Analysis

[3.1.](#) ILA

ILA is currently using a distributed key value (KV) store for identifier locator mapping [[I-D.herbert-ila-ilamp](#)]. The key value NoSQL database also supports publish/subscribe where the senders or publishers send the messages while the receivers or subscribers receive them and the link by which the messages are transferred is called channel. Such an approach avoids developing a request response protocol in order to update the mapping database with new identifier locator values or to access locator values for a given identifier and also leverages all the recent developments for security, availability, reliability, replication, etc. ILA

forwarding nodes (ILA-N) maintain caches of identifier locator values learned so far but these values are UE specific. The ILA Mapping Protocol (ILAMP) [[I-D.herbert-ila-ilamp](#)] is used between ILA forwarding nodes and ILA mapping routers (ILA-R). The purpose of the protocol is to populate and maintain the ILA mapping cache in forwarding nodes. ILA-N sends Map Request message to ILA-R with a list of identifiers and ILA-R replies with Map Information message with identifier to locator mappings. ILA-R contains a horizontal partition of the whole identifier locator database called a shard. LISP style request/response protocol based mapping system can also be used by ILA as defined in [[I-D.rodriqueznatal-ila-lisp](#)].

Privacy is addressed in the data plane by way of UE simultaneously using different addresses for different connections chosen from a block of addresses. It is observed that NAT can also provide address privacy but the use of NAT is discouraged in IETF. UE needs to reestablish connections every time it changes its address so address changing incurs delays which could be significant in case of real-time communication unless connections can be made simultaneously ('make before break').

[3.2.](#) LISP

In LISP, FQDN to identifier or EID mappings are stored in DNS. The LISP control-plane interface to the identifier-locator or EID-RLOC mapping system is defined in [[I-D.ietf-lisp-rfc6833bis](#)]. The LISP mapping transport system exists in three flavors: LISP-ALT [RFC 6836](#) [[RFC6836](#)] LISP NERD [RFC 6837](#) [[RFC6837](#)] and LISP-DDT [RFC 8111](#) [[RFC8111](#)], respectively. LISP data plane nodes, Ingress/Egress Tunnel Routers (ITR/ETR or xTR) registers mappings to the mapping system by sending Map-Register messages to the Map-Server(s). The Map Servers then publish these identifier locator values in the mapping system. There is Map-Resolver which accepts Map-Request messages from an ITR for the EID and returns the corresponding EID-to-RLOC-set mappings by consulting mapping database system in a Map-Reply message. All messages defined in the control plane are UDP messages. All read and write operations to the mapping system are authenticated with shared-keys using sha256 as well as ECDSA similar to DNSSEC as well as origin authentication, integrity and anti-replay protection [[I-D.ietf-lisp-sec](#)].

Note that ITRs keep a small scale identifier locator map of all values learned so far called a cache. In LISP mapping system, the lack of privacy support in the control plane for a given identifier value exists. On the data plane, LISP allows to encrypt identifiers [[RFC8061](#)]. Since ITR uses request/response exchange in getting the locator values, until a resolution response is received, packets for a flow may be blocked (like any other cache based solution), depending on the implementation policy. This means a Denial of Service attack on the ITR or cache has the worst case effect of indefinitely blocking a legitimate flow. Also the cache in ITR may raise privacy issue if EID-RLOC values for one UE is used for another UE. However, there are proposals for LISP to use a Publish/Subscribe approach [[I-D.rodriqueznatal-lisp-pubsub](#)]. While not yet explored, in the current LISP specification nothing prevents from using privacy addressing by way of UE simultaneously using different addresses for different connections chosen from a block of addresses in the data plane.

[4.](#) General Recommendations

The use of new type of databases known as NoSQL databases organized as Key-value stores or mapping systems is recommended. Such databases will provide very efficient read and writes unlike DNS. NoSQL mapping systems mostly support a message-oriented middleware system called publish-subscribe or PubSub. In PubSub, publishers are loosely coupled to subscribers and offer better scalability than traditional client-server systems because of parallel operation, message caching and network based message routing. Such systems support sharding based on a shard key across different database servers. Publish/subscribe mechanism takes cares of the request/response mechanism commonly used in DNS or other mapping systems and have better DDOS protection. Although a proposal exists as in [[I-D.herbert-ila-ilamp](#)], how such a Key-value store will be architected in 5GC is not defined. Some guidelines for sharding need to be developed. How the mapping database will be sharded based on its identifier values as the key differently for each Id-Loc system can be defined.

What is stored in the mapping system is limited to the identifier and locator values and no considerations to provide privacy of the stored

data.

There are many privacy improving mechanisms defined like locator/identifier privacy of frequent address changing of ILA, establishing and managing security associations between participating entities etc. Each of these techniques can be used by any Id-loc system. There is a need to standardize these privacy techniques in order to enable wide scale use by the end nodes.

[4.1.](#) Security In the Data Path

We address privacy problem for mapping systems: First we state the Atick privacy model which can be summarized as privacy at every levels. At the mapping system, the map data will be designed with privacy considerations so that the access will be enabled only for the allowed entities and disabled for any others. 5GC nodes/functions that are ingress/egress nodes may have caches and a protocol may be needed to communicate with other 5GC nodes that are part of the mapping servers and contains a shard. 5GC nodes/functions that are not ingress/egress nodes are considered part of the mapping servers and they provide secure access to the mapping data and may contain part of the mapping database. Privacy will be enabled in all 5GC nodes/functions that deal with the mapping database. Such considerations will be implemented by way of the privacy additions to the data stored in the mapping database. End hosts or UEs will be able to have control over their own mapping records stored in the

mapping database. End nodes or UEs that are unauthorized will not be able to have access to the location data of another UE. The same applies to the unauthorized entities or servers/functions in what 5G architecture calls outside data network (DN).

[5.](#) IANA Considerations

TBD.

[6.](#) Security Considerations

[7.](#) Acknowledgements

[8.](#) References

8.1. Normative References

- [I-D.ietf-lisp-rfc6830bis]
Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos-Aparicio, "The Locator/ID Separation Protocol (LISP)", [draft-ietf-lisp-rfc6830bis-12](#) (work in progress), March 2018.
- [I-D.ietf-lisp-rfc6833bis]
Fuller, V., Farinacci, D., and A. Cabellos-Aparicio, "Locator/ID Separation Protocol (LISP) Control-Plane", [draft-ietf-lisp-rfc6833bis-10](#) (work in progress), March 2018.
- [I-D.ietf-lisp-sec]
Maino, F., Ermagan, V., Cabellos-Aparicio, A., and D. Saucez, "LISP-Security (LISP-SEC)", [draft-ietf-lisp-sec-15](#) (work in progress), April 2018.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](#), DOI 10.17487/RFC4941, September 2007, <<https://www.rfc-editor.org/info/rfc4941>>.
- [RFC6836] Fuller, V., Farinacci, D., Meyer, D., and D. Lewis, "Locator/ID Separation Protocol Alternative Logical Topology (LISP+ALT)", [RFC 6836](#), DOI 10.17487/RFC6836, January 2013, <<https://www.rfc-editor.org/info/rfc6836>>.

- [RFC6837] Lear, E., "NERD: A Not-so-novel Endpoint ID (EID) to Routing Locator (RLOC) Database", [RFC 6837](#), DOI 10.17487/RFC6837, January 2013, <<https://www.rfc-editor.org/info/rfc6837>>.
- [RFC8061] Farinacci, D. and B. Weis, "Locator/ID Separation Protocol (LISP) Data-Plane Confidentiality", [RFC 8061](#), DOI 10.17487/RFC8061, February 2017,

<<https://www.rfc-editor.org/info/rfc8061>>.

- [RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", [RFC 8064](#), DOI 10.17487/RFC8064, February 2017, <<https://www.rfc-editor.org/info/rfc8064>>.
- [RFC8111] Fuller, V., Lewis, D., Ermagan, V., Jain, A., and A. Smirnov, "Locator/ID Separation Protocol Delegated Database Tree (LISP-DDT)", [RFC 8111](#), DOI 10.17487/RFC8111, May 2017, <<https://www.rfc-editor.org/info/rfc8111>>.

8.2. Informative References

- [I-D.herbert-ila-ilamp]
Herbert, T., "Identifier Locator Addressing Mapping Protocol", [draft-herbert-ila-ilamp-00](#) (work in progress), December 2017.
- [I-D.herbert-intarea-ila]
Herbert, T. and P. Lapukhov, "Identifier-locator addressing for IPv6", [draft-herbert-intarea-ila-01](#) (work in progress), March 2018.
- [I-D.ietf-intarea-tunnels]
Touch, J. and M. Townsley, "IP Tunnels in the Internet Architecture", [draft-ietf-intarea-tunnels-08](#) (work in progress), January 2018.
- [I-D.rodriqueznatal-ila-lisp]
Rodriguez-Natal, A., Ermagan, V., Maino, F., and A. Cabellos-Aparicio, "LISP control-plane for Identifier Locator Addressing (ILA)", [draft-rodriqueznatal-ila-lisp-01](#) (work in progress), April 2018.

Rodriguez-Natal, A., Ermagan, V., Leong, J., Maino, F., Cabellos-Aparicio, A., Barkai, S., Farinacci, D., Boucadair, M., Jacquenet, C., and S. Secci, "Publish/Subscribe Functionality for LISP", [draft-rodriqueznatal-lisp-pubsub-02](#) (work in progress), March 2018.

[I-D.xyz-atick-ps]

Hugo, D., Sarikaya, B., Iannone, L., and T. Herbert, "Problem Statement for Secure End to End Privacy Enabled Mapping System", [draft-xyz-atick-ps-00](#) (work in progress), May 2018.

[I-D.xyz-ideas-gap-analysis]

Qu, Y., Cabellos-Aparicio, A., Moskowitz, R., Liu, B., and A. Stockmayer, "Gap Analysis for Identity Enabled Networks", [draft-xyz-ideas-gap-analysis-00](#) (work in progress), July 2017.

Authors' Addresses

Dirk von Hugo
Deutsche Telekom
Deutsche-Telekom-Allee 7
D-64295 Darmstadt
Germany

Email: Dirk.von-Hugo@telekom.de

Behcet Sarikaya
Denpel Informatique

Email: sarikaya@ieee.org

Tom Herbert
Quantonium

Email: tom@quantonium.net

Luigi Iannone
Telecom ParisTech

Email: ggx@gigix.net