Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 15, 2019

D. von Hugo
Deutsche Telekom
B. Sarikaya
Denpel Informatique
L. Iannone
Telecom ParisTech
A. Petrescu
CEA, LIST
K. Sun
Soongsil University
U. Fattore
NEC

May 14, 2019

# Problem Statement for Secure End to End Privacy in IdLoc Systems
# draft-xyz-pidloc-ps-00.txt

Abstract

Efficient and service aware flexible end-to-end routing in future communication networks is achieved by routing protocol approaches making use of Identifier Locator separation systems. Since these systems require a correlation between identifiers and location which might allow tracking and misusage of individuals' identities and locations such operation demands for highly secure measures to preserve privacy of users and devices. This document tries to identify and describe typical use cases and derive thereof requirements to be fulfilled by privacy preserving Identifier-Locator split (PidLoc) approaches.

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 November 15, 2019.

Copyright Notice

Copyright (c) 2019 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 (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

Forthcoming future communication systems which are currently under specification by standardization organizations try to achieve higher resource efficiency and flexibility as compared to currently deployed and operated networks. Independent of specific access technologies multiple applications shall be served with different levels of policy- driven mobility support and quality of service in terms of bandwidth, latency, error probability etc. Current practice of IP address usage includes semantics as session identification as well as entity location and name resolution. Many networking and information processing related topics as cloud computing, software defined networking, network function virtualization, logical network slicing, and convergence of multiple heterogeneous access and transport

technologies call for new approaches towards service specific and optimized packet routing.

Promising proposals are Identifier Locator (Id-Loc) separation systems like Identifier Locator Addressing (ILA), Identifier-Locator Network Protocol (ILNP), Locator/ID Separation Protocol (LISP), and others.

Architectures and protocols for these approaches are already documented in detail and are under continuous evolution in different WGs. This document on the other hand attempts to identify potential issues with respect to real-world deployment scenarios which may demand for light- weight implementations of Id-Loc systems. Especially the issues related to threads due to privacy violation of devices and their users as well as location detection and movement tracking may demand for specific countermeasures.

To provide a problem statement this draft documents common aspects and differences of several Id-Loc approaches from a high-level perspective and describes a set of use cases resulting in identified requirements towards privacy and security.

## 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].

Identifier: An identifier is information to unambiguously identify an entity or an entity group within a given scope. An identifier is the equivalent of an End point identifier (EID) in The Locator/ID Separation Protocol (LISP). It may be visible in communications.

Locator: A locator is a routable network address. It may be associated with an identifier and used for communication on the network layer according to identifier locator split principle. A locator is the equivalent of a Routing Locator (RLOC) in LISP or an IP address in other cases.

## 3. Identifier Locator Separation Protocols

Identifier represents a communication end-point of an entity and may not be routable. Locator also represents a communication end point, i.e. its routable network address and thus can change if the entity moves. A database called a mapping system needs to be used for identifier to locator mapping. Identifiers are mapped to locators for forwarding purposes. Mapping system has to handle mobility by modifying identifier to locator mappings in the database.

To start the communication, a device needs to know the identifier of the destination and then relies on a process to lookup on a network identifier and return the locator(s). Note that both identifier and locator can be carried in clear in packet headers.

Usage of identifiers readily available for public access raises privacy issues. For public entities, it may be desirable to have their fully qualified domain names or host names available for public lookups by the clients however such is not the case in general for the identifiers, e.g. for individuals roaming in a mobile network.

ILNP

Identifier-Locator Network Protocol (ILNP) [RFC6740] is a host- based approach enabling mobility using mechanisms that are only deployed in end-systems and do not require any router changes. ...

ILA

Identifier-Locator Addressing (ILA) [I-D.herbert-intarea-ila] uses address transformation proposing to split an IPv6 address in 64-bit identifier (lower address bits) and locator (higher address bits) portions. The locator part is determined dynamically from a mapping table that maintains associations between the location-independent identifiers and topologically significant locators. ...

LISP

Locator/Id Separation Protocol (LISP) [RFC6830] is a network based approach using mapping and encapsulation of packets proposing a LISP architecture which provides a level of indirection for routing and addressing performed at specific ingress/egress routers at the LISP domain boundaries. LISP control plane protocol [RFC6833] can also be applied to various other user plane protocols. Both LISP user plane as control plane are under revision as [I-D.ietf-lisp-rfc6830bis] and [I-D.ietf-lisp-rfc6833bis], respectively. ...

## 4. Use Cases

The collection of use cases shall serve as starting point to derive requirements to future solutions providing privacy and security in generic Identifier Locator Split Approaches.

### 4.1. Industrial IoT

Sensors and other connected things in the industry are usually no personal items (e.g. wearables) potentially revealing an indiduals sensitive information but business assets which should be detected

only by authorised intra-company entities. Since the huge amount of these things (massive IoT) as well as typical energy and bandwidth constraints of battery-powered devices may pose a challenge to traditional routing and security measures privacy enabled Id-Loc split approaches are proposed as a viable approach here, [I-D.nordmark-id-loc-privacy] ...

### 4.2. 5G Use Case

Upcoming new truely universal communication via so-called 5G systems will demand for much more that (just) higher bandwidth and lower latency. Integration of heterogeneous multiple access technologies (both wireless and wireleine) controlled by a common converged core network and the evolution to service-based flexile functionalities instead of hard-coded network functions calls for new protocols both on control and user (data) plane. While Id-Loc approach would serve well here the challenge to provide a unique level of security and privacy even for a lightweight routing and forwarding mechanism - allowing for ease of deployment and migration from existing operational network architecture - remains to be solved.

### 4.3. Cloud Use Case

The cloud, i.e. a set of distributed data centers for processing and storage connected via highspeed transmission paths, is seen as logical location for content and also for virtualized network function instances and shall provide measures for easy re-location and migration of these instances deployed as e.g. containers or virtual machines. Id-Loc split routing protocols are proposed for usage here while the topology of the cloud components and logical correlations shall be invisible from outside. ...

### 4.4. Vehicular Networks

In vehicular networks use cases (e.g. for a future C-ITS, i.e. Cooperative Intelligent Transport Systems) there are some problems related to privacy. Cars are mandated to beacon CAM messages (cooperative awareness message - also denoted as basic service message, BSM) very frequently (more than 1 per second). These messages contain identifiers such as MAC addresses. They are unique and visible in the public oui.txt file. They can be tracked. But these are MAC addresses, not IP addresses.

If, in the future, cars beacon Router Advertisements as well, then there is a risk in the src address of these RAs - the LL. They are usually formed out of the MAC address, even though recent RFC7217 [RFC7217] give suggestion of using a random ID in the IID (Interface Identifiers) (rather than the MAC address); the RFC stays silent

about the prefix length; since the RFC7217 method covers also the LL addresses, and requires them to be RFC4291-like (64bit length), that random ID is still of fixed length (64). Longer than 64 IIDs may benefit privacy, since crypto attacks on them would be harder.

A variable length IID in link-local addresses may help create a flexible identifier-locator split thus increasing privacy.

In addition C-ITS shall also allow to improve vehicular network based services as e.g. predict traffic congestion along the route and propose a re-direction towards alternative routes, or predict network coverage along the foreseen path to adapt a critical service. This on the other hand demands for knowledge of the actual route, i.e. tracking of the vehicle. As was shown in [NYC_cab] even anonymizing sometimes does not prevent from privacy breaches. ...

## 5. PIdLoc Requirements

TBD.

## 6. IANA Considerations

TBD.

## 7. Security Considerations

## 8. Acknowledgements

## 9. References

### 9.1. 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-26 (work in progress), November 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-24 (work in progress), February 2019.

[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>.

## 9.2. Informative References

[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-09 (work in progress), July 2018.

[I-D.ietf-lisp-sec]
Maino, F., Ermagan, V., Cabellos-Aparicio, A., and D. Saucez, "LISP-Security (LISP-SEC)", draft-ietf-lisp-sec-17 (work in progress), November 2018.

[I-D.nordmark-id-loc-privacy]
Nordmark, E., "Privacy issues in ID/locator separation systems", draft-nordmark-id-loc-privacy-00 (work in progress), July 2018.

[NYC_cab] Douriez, et al., M., "Anonymizing NYC Taxi Data: Does It Matter?", Proc. of IEEE Intl. Conf. on Data Science and Advanced Analytics (DSAA'16) , pp. 140-148, 2016.

[RFC6740] Atkinson, RJ. and SN. Bhatti, "Identifier-Locator Network Protocol (ILNP) Architectural Description", RFC 6740, DOI 10.17487/RFC6740, November 2012, <https://www.rfc-editor.org/info/rfc6740>.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <https://www.rfc-editor.org/info/rfc6830>.

[RFC6833] Fuller, V. and D. Farinacci, "Locator/ID Separation Protocol (LISP) Map-Server Interface", RFC 6833, DOI 10.17487/RFC6833, January 2013, <https://www.rfc-editor.org/info/rfc6833>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

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

Luigi Iannone
Telecom ParisTech

Email: ggx@gigix.net

Alex Petrescu
CEA, LIST

Email: alexandre.petrescu@gmail.com

Kyoungjae Sun
Soongsil University

Email: gomjae@dcn.ssu.ac.kr

Umberto Fattore
NEC

Email: Umberto.Fattore@neclab.eu