

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 5, 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
June 3, 2019

Problem Statement for Secure End to End Privacy in IdLoc Systems
draft-xyz-pidloc-ps-02

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 misuse 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 a problem statement describing issues and challenges for application of 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 December 5, 2019.

Internet-Draft

Pidloc Problem Statement

June 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	2
2.	Conventions and Terminology	3
3.	Identifier Locator Separation Protocols	4
3.1.	ILNP	4
3.2.	ILA	4
3.3.	LISP	5
3.4.	Privacy in IdLoc Protocols	5
4.	Use Cases	6
4.1.	Industrial IoT	6
4.2.	5G Use Case	6
4.3.	Cloud Use Case	7
4.4.	Vehicular Networks	7
5.	PIdLoc Issues and Challenges	8
6.	IANA Considerations	8
7.	Security Considerations	8
8.	Acknowledgements	8
9.	References	8
	Authors' Addresses	10

[1.](#) Introduction

Forthcoming future communication systems which are currently under specification by various SDOs (Standards Development 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) [[I-D.herbert-intarea-ila](#)], Identifier-Locator Network Protocol (ILNP) [[RFC6740](#)], Locator/ID Separation Protocol (LISP) [[I-D.ietf-lisp-rfc6830bis](#)] [[I-D.ietf-lisp-rfc6833bis](#)], 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 implementations of the above-mentioned Id-Loc systems. In particular, this document focuses on issues related to threats due to privacy violation of devices and their users, as well as location detection and movement tracking, where specific countermeasures may be needed.

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 issues and challenges concerning privacy and security. A set of requirements as outcome of a detailed analysis of these both generic and use cases specific questions will be provided in a companion document.

[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 allowing 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 or may not 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, however, it is a routable network address. Because entities identified by an Identifier can move the association between Identifiers and Locators may be ephemeral. A database called a mapping system needs to be used for Identifier to Locator mapping. Identifiers are mapped to locators for reachability purposes. A mapping system has to handle mobility by updating the identifier to locator mappings in the database.

To start the communication, a device needs to know the identifier of the destination, hence it relies on a identifier lookup process to obtain the associated locator(s). Note that both identifier and locator may be carried in clear in packet headers, depending on the specific technology used and the level of security/privacy enforced.

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, this is not the case in general for all identifiers, e.g. for individuals roaming in a mobile network.

[3.1.](#) 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.

[3.2.](#) 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.

ILA is currently deployed in commercially available cloud systems such as Facebook and Google which are Layer 3 based. Also A kernel implementation of ILA is available in Linux distribution. ILA does not require any transport layer (UDP/TCP) changes.

von Hugo, et al.

Expires December 5, 2019

[Page 4]

Internet-Draft

Pidloc Problem Statement

June 2019

[3.3.](#) LISP

Locator/Id Separation Protocol (LISP) [[I-D.ietf-lisp-rfc6830bis](#)] [[I-D.ietf-lisp-rfc6833bis](#)] is based on a map-and-encap approach, which provides a level of indirection for routing and addressing performed at specific ingress/egress routers at the LISP domain boundaries. Such border routers performing LISP encapsulation at the packet's source stub network are indicated as Ingress Tunnel Routers (ITRs), while border routers at the packet's destination stub network are called Egress Tunnel Routers (ETRs), all of them are indicated by the general term xTRs. In order to obtain mappings used for encapsulation operation, xTRs query the mapping system in order to obtain all mappings related to a certain EID only when necessary (usually, but not exclusively, at the beginning of a new flow transmission). The LISP control plane protocol [[I-D.ietf-lisp-rfc6833bis](#)] allows to support several different mapping systems (e.g., LISP+ALT [[RFC6836](#)] and LISP-DDT [[RFC8111](#)]). More than that, it can actually also be applied to various other data plane protocols.

[3.4.](#) Privacy in IdLoc Protocols

In all of the above protocols of ILNP, ILA and LISP, the identifiers are carried in packet headers in clear and therefore preserving identifier's privacy is needed. Otherwise private information such as the location and content of the communication can be revealed.

In case of ILNP, public DNS can be used to by the end nodes to access the destination identifier for a given Fully Qualified Domain Name (FQDN). However the same node also gets the locator values raising serious privacy issues in the control plane. As for the data plane, both source locator and identifier need to be privacy protected and techniques such as locator rewriting and ephemeral-use identifiers, respectively are suggested.

In the control plane, ILA exhibits similar privacy issues if the ILA mapping system defining identifier locator mappings can publicly be accessed. In ILA, privacy is addressed in the data plane by way of UE simultaneously using different addresses for different connections chosen from a block of addresses.

In LISP mapping system, the lack of privacy support in the control plane for a given identifier value exists due to the use of DNS, as in ILNP. In the data plane, privacy addressing by way of UE simultaneously using different addresses for different connections chosen from a block of addresses can be used as in ILA.

[4.](#) Use Cases

The collection of use cases shall serve as starting point to identify different issues and challenges allowing for later derivation of 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 not personal items (e.g. wearables) potentially revealing an individual's sensitive information. Yet, industrial connected objects are business assets which should be detected/accessed only by authorised intra-company entities. Since the huge amount of these things (massive IoT) as well as the 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](#)].

In Industrial IoT, there are very strong reasons to not share the ID/ Locator binding with third parties, i.e. retain the privacy. This can be achieved in a number of ways such as: using an ID/locator system but using some fixed anchor points a locator; injecting routing prefixes for the ID prefixes into the normal routing system and use proxy indirection; providing limited ID/Locator exposure. These are just examples, more approaches should be explored in order to find which one is the most suitable in the context of industrial IoT.

[4.2.](#) 5G Use Case

Upcoming new truly universal communication via so-called 5G systems will demand for much more than (just) higher bandwidth and lower latency. Integration of heterogeneous multiple access technologies (both wireless and wireline) controlled by a common converged core network and the evolution to service-based flexible 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 high speed 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 as in ILA [[I-D.herbert-intarea-ila](#)] and LISP [[I-D.ietf-lisp-rfc6830bis](#)] [[I-D.ietf-lisp-rfc6833bis](#)] while the topology of the cloud components and logical correlations shall be invisible from outside.

In a cloud, an upstream IP address does not necessarily belong to the actual service location, but a gateway or load balancer. So, the locator or also ID reveal the location with the accuracy of a data center, not the function taking a service request. This issue also manifests itself in today's LTE as PGWs are in a data center binding UEs' IP addresses which are from the network of the data center.

[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 source address of these RAs - the link local (LL) address. 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. ...

Strong access control to ID/LOC mapping system(e.g. using longer and variable length of IID, crypto-ID, etc.) has some tradeoffs between enhancing privacy and increasing delay. Furthermore, in the vehicular network, reducing delay is also very important issue because vehicle moves too fast to have enough time to configure.

For V2V communication, using temporary identifier between two vehicles can be one solution to prevent privacy. When we think of the example for V2V communication, most of their data includes current traffic condition, speed, or accident information which are not related to identify their unique device information.

[[I-D.ietf-lisp-eid-anonymity](#)] can be one good solution to provide anonymity. In [[I-D.ietf-ipwave-vehicular-networking](#)], they suggest MAC address pseudonym in which MAC address is changed periodically.

[5.](#) PIdLoc Issues and Challenges

This section concludes on both common and specific issues and challenges in PIdLoc to allow for derivation of requirements to potential solutions serving for a gap analysis to be documented in upcoming drafts, e.g. (I-D.xyz-pidloc-reqs).

[6.](#) IANA Considerations

TBD.

[7.](#) Security Considerations

TBD

[8.](#) Acknowledgements

[9.](#) 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-ipwave-vehicular-networking]

Jeong, J., "IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", [draft-ietf-ipwave-vehicular-networking-09](#) (work in progress), May 2019.

[I-D.ietf-lisp-eid-anonymity]

Farinacci, D., Pillay-Esnault, P., and W. Haddad, "LISP EID Anonymity", [draft-ietf-lisp-eid-anonymity-06](#) (work in progress), April 2019.

[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.

[I-D.ietf-lisp-sec]

Maino, F., Ermagan, V., Cabellos-Aparicio, A., and D. Saucez, "LISP-Security (LISP-SEC)", [draft-ietf-lisp-sec-18](#) (work in progress), June 2019.

[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.

[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>>.

[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>>.

Internet-Draft

Pidloc Problem Statement

June 2019

- [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>>.
- [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>>.
- [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>>.

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

von Hugo, et al.	Expires December 5, 2019	[Page 10]
------------------	--------------------------	-----------

Internet-Draft	Pidloc Problem Statement	June 2019
----------------	--------------------------	-----------

Kyoungjae Sun
Soongsil University

Email: gomjae@dcn.ssu.ac.kr

Umberto Fattore
NEC

Email: Umberto.Fattore@neclab.eu

von Hugo, et al.

Expires December 5, 2019

[Page 11]