Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 28, 2019

L. Iannone
Telecom ParisTech
D. von Hugo
Deutsche Telekom
B. Sarikaya
Denpel Informatique

May 27, 2019

Requirements to Secure End to End Privacy in IdLoc Systems
draft-xyz-pidloc-reqs-00.txt

Abstract

Use of Identifier Locator separation systems is proposed for various use cases to allow for efficient and service aware flexible end-to-end routing. A statement on the issue of privacy preservation of both users and devices identity and location describes major challenges identified for this problem. This document attempts to derive requirements towards a potential solution space of approaches to preserve privacy in Identifier-Locator split (PidLoc) protocols.

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 28, 2019.

Table of Contents

1. Introduction

[I-D.xyz-pidloc-ps] has identified and described typical use cases for application of privacy preserving Identifier-Locator split (PidLoc) approaches and derived thereof a problem statement describing corresponding issues and challenges. Privacy in this respect includes prevention of acquisition of personal information, behavioral details, and location information by unauthorised parties. This document tries to assess that set of issues and challenges to come up with a set of requirements for approaches towards service specific and optimized packet routing based on Id-Loc principle providing 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] and [I-D.xyz-pidloc-ps].

3. Identifier Locator Separation Protocols

This section summarizes the specifics and commonalities of existing Identifier Locator (Id-Loc) Separation Protocols and highlights the corresponding challenges and issues identified in [I-D.xyz-pidloc-ps].

4. PId-Loc Requirements

This section lists requirements which emerge from the use case analysis and will apply (beside the general requirements to fit with privacy considerations for Internet Protocols as laid down in RFC 6973 [RFC6973] and partly also on design criteria for confidentiality in the data plane of LISP described in RFC 8061 [RFC8061]) for the solution space providing privacy and security in generic Identifier Locator Split Approaches.

4.1. Limited Effort

The measures to ensure privacy to Id-Loc systems shall not require additional infrastructure and external third party provided resources to be used nor increase the overall effort such that network and service performance is strongly degraded. Successful privacy measures shall not impact availability.

4.2. Flexibility

Because Id-Loc approaches can be used in mobile environments, flexibility in time and space should be provided. The same Id, associated to a specific device, can move around and at different times can have different privacy requirements, may be depending on the specific connection or provider used. Still because of mobility, a certain device can have different privacy requirements depending of where it is.

4.3. Scalability

Because some of the ID-Loc proposals aim at being deployed in datacenters, the methods to ensure privacy has to be able to function at very large scale.

4.4. Resiliency

The measure shall not rely on a potential single point of failure nor a single mechanism and allow for automatic rebooting or relying on alternative solutions in case of compromise and attacks.

4.5. ID to Locator Association Protection

The Id-Loc system may need to use measures for binding one or more identifiers to one or more locators. This is usually achieved by a mapping or lookup system (e.g. DNS) which has to be protected against unauthorised access and may allow for different policy-based chosen levels of security. Like any other software-based service, the mapping system has to be protected against DDoS attacks and the like. However, there are specific points to be tackled:

- Mapping System Access Control: Who can access the mapping system?
- Mapping Access Control: Someone authorized to access the mapping system does not mean that is authorized to access the mapping of a specific Identifier.
- Byzantines Attacks: What if someone is able to inject tempered information to attack either the mapping system itself of a specific identifier?

The above may be defined on various criteria, like for instance administrative criteria "devices part of the same company", or geographical criteria "only close by devices", or service-aware "devices operating the same service".

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-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>.

8.2. 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.

[I-D.xyz-pidloc-ps]
Hugo, D., Sarikaya, B., Iannone, L., Petrescu, A., Kj, S., and U. Fattore, "Problem Statement for Secure End to End Privacy in IdLoc Systems", draft-xyz-pidloc-ps-00 (work in progress), May 2019.

[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>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <https://www.rfc-editor.org/info/rfc6973>.

[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>.

[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>.

Authors' Addresses

Luigi Iannone
Telecom ParisTech

Email: ggx@gigix.net

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