

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

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

Problem Statement for Secure End to End Privacy Enabled Mapping System
draft-xyz-atick-ps-01.txt

Abstract

Problem Statement for Secure End to End Privacy Enabled Mapping System for Identifier Locator separation systems is presented. Since identifiers are often carried in packet headers in clear, and mapping systems are often designed to be accessible by any entity, to preserve identifier's privacy, lookups to the mapping system should be allowed only by authorized entities. In mapping systems, in addition to privacy, security also requires special attention because of the caches introduced into the data path. Any denial of service attacks on the cache should not allow the communication to come to an end.

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.

Internet-Draft

Atick Problem Statement

June 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 (<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.	Problem Statement	3
3.1.	Security In the Data Path	5
4.	IANA Considerations	5
5.	Security Considerations	5
6.	Acknowledgements	5
7.	References	5
7.1.	Normative References	6
7.2.	Informative References	6
	Authors' Addresses	7

[1.](#) Introduction

Current 4G and the upcoming converged communication network of 5G core network (5GC) make use of tunneling with anchor points to handle mobility, policy and quality of service. The use of IP addresses induces the topology and enables easy location tracking. Elimination or reduction of anchor points, as well as disassociating topology from IP addresses to facilitate efficient mobility and user privacy using Identifier Locator separation systems like Identifier Locator Addressing, The Locator/ID Separation Protocol and others is needed. Many drawbacks of tunneling are discussed in [\[I-D.ietf-intarea-tunnels\]](#) and we do not repeat them here.

This document attempts to make the case for the use of the identifier

locator separation (Id-Loc) protocols in the data plane and identifies the problems for such a large scale use. The problems identified mainly are privacy of the identifiers and associated locators and security issues.

[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.](#) Problem Statement

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.

This document describes the problem statement for a new kind of mapping system to be used by identifier locator separation systems (Id-Loc) that are end to end privacy enabled.

Heavy use of tunneling with fixed anchors:

Current 4G and the upcoming converged communication network of 5G core network (5GC) make use of tunneling with anchor points to handle mobility, policy and quality of service. The use of IP addresses induces the topology and enables easy location tracking. Elimination

or reduction of anchor points, as well as disassociating topology from IP addresses to facilitate efficient mobility and user privacy using Identifier Locator separation systems is needed. 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 which is required to support mobility. Added complexity of increased signaling for tunnel management are further drawbacks [[I-D.ietf-intarea-tunnels](#)].

Proposed 5G operation:

The use of GTP is proposed to tunnel UE packets from the base station, gNB to the User Plane Function (UPF) in N3 interface establishes a fixed anchor for UE traffic and UPF further GTP tunnels to another UPF in N9 interface which is connected to an external data network (DN). Access and Session Management control plane functions (AMF, SMF) push such configuration setup to the data plane functions. With such a rigid setup user mobility as well as UE receiving traffic on multiple interfaces can not be handled efficiently. UE to another UE traffic has to go to the fixed anchor since gNBs are not mobility anchors. Also due to the induced delays, delay sensitive applications such as Ultra Reliable Low Latency (URLL) applications can not be supported.

IP Addressing Reveals geographic location:

Addressing scheme in use currently reveal the topology of the internet and thus location privacy of the end nodes can not be

established. Move away from this heavy use of locators is needed in favor of identifier locator separation systems.

Gap Analysis:

Gaps in mapping solutions developed so far in Id-Loc systems reveal the fact that secure end to end privacy enabled mapping system approach is needed across the board [[I-D.xyzy-atick-gaps](#)].

Access to a mapping system should not reveal the location about an entity to the unauthorized requestor of a look up on an identifier. Tracking of the identifiers of an entity and mounting attacks based on that should be avoided. On the other hand discovery by the entities that are allowed to should not be made difficult. This may be possible by using encryption effectively in the control plane mechanisms to avoid eavesdroppers to access such information [[I-D.ietf-lisp-sec](#)].

If locators/ addresses (or device prefixes) are common between flows for a given entity then a third party can make inferences (i.e. whether they are sourced from the same host). This points to the problem of persistent identifiers which should be avoided.

Compromise of a mapping system is very bad since it would allow attackers to take control of traffic and to misdirect it.

If locators/ addresses contain fine grained topology then device location (and hence user location) can be inferred. This gets to the problem that locators may contain detailed geographic location information and hence are very sensitive data. This points to the need for using identifier locator separation.

Scaling is an issue for mapping systems built using very high performance massively distributed noSQL databases. Slow moving or fixed hosts can probably induce light loads on mapping systems. In 5G case, very high number of devices moving at high speeds this changes drastically, i.e. very heavy load is induced on the mapping system. Mapping systems that scale to 100s of millions of entries with 100s of milliseconds response times are needed. State of the art shows that such systems can be built and operated with the use of

thousands of servers worldwide.

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

If a cache is introduced into the data path (as might be the case in some mapping systems) then that in turn will introduce potential DoS attacks in order to slow down or even completely stop the communication. So proper protocol actions and security policies should be taken against DoS attacks.

Compromise of a mapping system is very bad since it would allow attackers to take control of traffic and to misdirect it.

[4.](#) IANA Considerations

TBD.

[5.](#) Security Considerations

[6.](#) Acknowledgements

[7.](#) References

von Hugo, et al. Expires December 9, 2018 [Page 5]

Internet-Draft Atick Problem Statement June 2018

[7.1.](#) 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.

[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>>.

7.2. 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-08](#) (work in progress), January 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.
- [I-D.xyzy-atick-gaps]
Hugo, D., Sarikaya, B., Herbert, T., Iannone, L., and S. Bhatti, "Gap and Solution Space Analysis for End to End Privacy Enabled Mapping System", [draft-xyzy-atick-gaps-00](#) (work in progress), May 2018.

von Hugo, et al.

Expires December 9, 2018

[Page 6]

Internet-Draft

Atick Problem Statement

June 2018

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

Tom Herbert
Quantonium

Email: tom@herbertland.com