Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 4, 2018

Y. Qu, Ed.
Huawei
A. Cabellos
Technical University of Catalonia
R. Moskowitz
HTT Consulting
B. Liu
Huawei
A. Stockmayer
University of Tuebingen

July 3, 2017

Gap Analysis for Identity Enabled Networks
draft-xyz-ideas-gap-analysis-00

Abstract

Currently there are several identifier/locator separation protocols, such as HIP, ILA, ILNA and LISP. This document analyzes the technical gaps between existing solutions and today's privacy requirements.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The separation of location and identifier has been discussed for many years, as documented in [RFC4984]. IP addresses have been overloaded to serve as both locators and identifiers. Several identifier and locator separation (ID/LOC) protocols have been proposed, such as HIP [RFC7401], [ILA] and LISP [RFC6830]. They create two separate namespaces: identifiers (IDfs) and Locators (LOCs). Identifiers uniquely identify network entities no matter where they are located, and locators are assigned based on topology information and are typically routable.

In an ID/LOC protocol, a service is needed to maintain mappings between identifiers and locators and to perform lookups from identifiers to locators (and probably vice-verse). Currently each ID-based protocol uses its own mapping database and mechanism to get this mapping information [RFC6836][RFC8005].

As pointed out by [IDEAS-PS][IDEAS-IDY-USE], the concept of identity (IDy) tied to a network entity can help to solve some of the privacy issues that are associated with today's networks. The goal of this document is to analyze the technical gaps between the existing ID/LOC protocols and today's requirements. The following gaps are summarized: the split of identifier and identity; a common mapping system supporting both IDf/LOC mapping and IDy/IDf mapping; and user-defined access policies.

2. Specification of Requirements

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 [RFC2119].

3. Definition of Terms

This document makes use of the terms that have been already defined in the problem statement draft of IDEAS [IDEAS-PS]. They are included here for reader's convenience. In case of any discrepancies between the two drafts, the problem statement draft overrides.

Entity: An entity is a communication endpoint. It can be a device, a node, or a virtual machine (VM), that needs to be identified. An entity may have one or multiple identifiers (long-lived or ephemeral) simultaneously. An entity is reached by the resolution of one or more of its identifiers to one or more locators.

Identity (IDy): the essence of "being" of a specific entity. An identity is not to be confused with an identifier: while an identifier may be used to refer to an entity, an identifier's lifecycle is not necessarily tied to the lifecycle of the Identity it is referencing. On the other hand, the identity's lifecycle is inherently tied to the lifecycle of the entity itself.

Identifier (IDf): denotes information to unambiguously identify an entity within a given scope (e.g. HIP HIT, LISP EID). There is no constraint on the format, obfuscation or routability of an IDy. The IDy may or may not be present in the packet whose format is defined by ID-based protocols (HIP/LISP).

Identifier-based (ID-based): When an entity is only reachable through one or more communication access then a protocol or a solution is said to be ID-based if it uses an ID-LOC decoupling and a mapping system (MS) as base components of the architecture. Examples of ID-based protocols are HIP, LISP and ILA.

IDentity Enabled Networks (IDEAS): IDEAS are networks that support the identifier/locator decoupling. Reaching an entity is achieved by the resolution of identifier(s) to locator(s).

Locator (LOC): denotes information that is topology-dependent and which is used to forward packets to a given entity attached to a network (IPv4/IPv6/L2/L2.5 Address). An entity can be reached using one or multiple locators; these locators may have a limited validity lifetime.

ID/LOC: Identifier and Locator Separation.

LISP: Locator/ID Separation Protocol.

HIP: Host Identity Protocol.

ILNP: Identifier-Locator Network Protocol.

ILA: Identifier-Locator Addressing.

DNS: Domain Name System.

4. Overview of ID/LOC Protocols

4.1. LISP

The Locator/ID Separation Protocol (LISP) [RFC6830] is structured around four main components: the data plane, the control plane (both specified in [RFC6830]), the LISP Mapping System Interface [RFC6833] and the Mapping System (e.g., LISP-DDT [RFC8111] and LISP+ALT [RFC6836]).

The LISP architecture decouples identifier and locator by means of the mapping system interface. This well-defined interface separates data/control from the mapping system architecture. As a result, LISP does not assume any mapping system architecture. The LISP WG has, at the time of this writing, specified two mapping systems: LISP-DDT [RFC8111] and LISP-ALT [RFC6836].

Both mapping system assume hierarchical identifiers, but the WG has explored other architectures such as DHT for flat identifiers, or monolithic mapping systems.

One of the main design principles behind LISP is to decouple the identifier (EIDs) from the locators (RLOCs). By means of the LISP Canonical Address Format (LCAF) [RFC8060] LISP provides a flexible syntax to encode both EIDs and RLOCs.

In terms of security, LISP supports authorization for mapping updates and the authentication of the clients updating such information. This is achieved by means of the authentication data field in the Map-Register message. In addition, LISP clients can verify the security of data origin, authentication and delegation. This is specified in [LISP-SEC] and the security mechanisms incorporated in LISP-DDT [RFC8111].

4.2. HIP

The Host Identity Protocol (HIP) [RFC7401] is a SIGMA-security compliant exchange of current entity location for a pair of cryptographically ownership provable Identifiers (HITs). HIP is, at its inception, focused on the management of the Identifier/Location mapping. HITs are valid, non-routable IPv6 addresses that carry the cryptographic protocol suite and a hash of the HI (Host Identity public key).

One method of discovery of a peer's HIT and initial location is either via DNS RR 55 [RFC8005] with A|AAAA RR to the peer or A|AAAA RR pointing to the peer's Rendezvous Service (RVS) server [RFC8004]. The Initiating peer cannot detect from DNS the difference in destination. The RVS server "slingshots" the I1 packet to the recipient. The recipient decides, based on local policy, to respond with the next exchange packet, R1. Thus using an RVS server not only supports client mobility, it also hides a peer's location unless it wants to be 'found'.

HIP provides Identity/Location separation through changes in the peer IP stack behavior with only needing RVS added to the infrastructure. HIP aware systems register to their RVS server(s) via a HIP exchange, augmented with an RVS registration parameter [RFC8003]. All location changes are made securely over HIP [RFC8046]. Location changes are sent directly to peers and to the RVS server(s). HIP fully supports double jumps (both peers move) and state lose recovery (full protocol state machine).

HIP supports multihomed systems [RFC8047], fully decoupling Identifier (HITs) from all interfaces. Multiple data-paths are enabled with HIP. ESP via BEET mode [rfc7402] is most commonly used. L2VPNs support is defined in [HIP-VPLS] and provided in commercial products targeting SCADA environments. A non-cryptographic envelope is proposed [HIP-IP].

HIP works equally well over IPv4 or IPv6 networks. The HIP data-path can be either IPv4 (via the HIP 32-bit Local Scope Identifier) or IPv6 using the HIT. IPv4 applications can run transparently over IPv6 and IPv6 over IPv4.

HIP well supports Identifiers to location, and weakly Identity to Identifiers. Besides DNS support, identities may be supported in HIP with X.509 certificates [rfc8002] to provide 3rd party assertions of HITs and HIs. Identifiers to Identity reversal is poorly handled, though potentially needed for support of FTP PASV and other protocols with embedded addresses. DHT has been demonstrated [RFC6537], but not fielded. The new work on Hierarchical HITs [HHIT] proposes new methods to couple DNS and a registry for the reverse lookup.

4.3. ILA

In [ILA], an IPv6 address is divided into two parts: a locator and an identifier. As other ID/LOC protocol, the locator indicates the topological location of a network entity, and the identifier identifies the entity in communications. ILA can be used to implement overlay networks for network virtualization, and also addresses use cases in mobility.

However, the mapping service in ILA is still TBD [ILA-MS-TBD].

5. Gap Analysis

5.1. The Split of Identity and Identifier

In existing ID/LOC Protocols, the IDf/LOC mappings stored in the mapping system are assumed to be public. A legitimate requestor can lookup any record, and escape access control policy, if there is any, by changing to a different identifier. Also a network entity may want to hide its true identity for privacy protection by using ephemeral identifiers [LISP-ANNOY].

To address these issues, [IDEAS-PS] introduces the concept of identity (IDy). An IDy uniquely identifies "who" is a communication entity. Identifier and locator together identifies "where" is the entity. With this 2-tier identification, multiple identifiers can be bound to the same entity (IDy) and exchanged in clear on the wire, without having to worry about the identity being compromised by outside observers.

Since the lifecycle of an identity is the same as the entity, the lifecycles of identity and its associated identifiers are decoupled. It is possible for identifiers to be added or removed without affecting the identity. This further abstraction can bring additional benefits. [IDEAS-IDY-USE] describes the identity use cases.

In summary:

- The notion of identity is not adequately supported.

- Two tiers of identification are needed, with identifiers anchored at the identity.

5.2. A Common Identifier-to-Locator Mapping System

IDf/LOC mapping service is essential for ID/LOC protocols [RFC6833], however now each protocol is using its own mapping database even within the same administrative domain. This potentially adds additional operational cost and management complexity.

A common mapping system supporting both IDf/LOC mapping and IDy/IDf mapping can work with existing ID/LOC protocols, as well as add extra identity based services. It can provide consistent access control, common interface for services such as registration, discovery and resolution. A unified database can help to ease network management [IDEAS-PS].

5.3. User-Defined Access Policies in the Mapping System

Different from DNS, which generally maintains public name-to-IP mapping information, an IDf/LOC mapping system maintains more private information. However existing mapping systems assume the information stored is public, and this may cause privacy violation. A network entity may want to set a customized access policy to control who can get its identifier and location information. This policy should be tied to identity, so it is not affected by identifier changes of the requestor.

General system-wide access control (e.g., an operator can set a system-wide access control list for a DNS server, only permitting the customer network prefixes to access it) can provide some privacy, but it is not sufficient. What is needed are: fine-grained level of access control at the level of data records associated with each individual entity; and reinforcement of the access policies.

6. Analysis of DNS

Since the 1980s, DNS has been pivotal to translate human readable names that are easy to remember into hard-to-remember IP addresses. It provides a global distributed directory service and is a very powerful and useful technology to translate the domain name hierarchy to IP address space.

Even though the DNS was designed to be resilient, it is prone to DDOS attacks as discussed extensively in the Technical Plenary of IETF97. Furthermore, some studies have also described challenges in the

response time and caching techniques and latency in the Internet [DNS1] [DNS2] [DNS3] [GNRS].

[DNS-DUP] proposed a mobility solution using DNS dynamic updating protocol. However for a communication session when both hosts are moving, the session fails and the hosts SHOULD query DNS and get the new address and then restart the communications.

The use of a mapping system rather than using DNS system has been discussed extensively in [IVIP], [RFC6115], on the lisp-wg mailing list [LISP-DIS], and initial HIP design team (circa 1999-2003).

7. Security Considerations

IDEAS control plane may be used to maintain and transmit confidential data, such as identity, access policy and metadata. Access to the data needs to be authorized/authenticated. Control plane messages containing such data need to be encrypted. The exact details of encryption/authentication are topics for future research.

8. IANA Considerations

This document has no actions for IANA.

9. Contributors

TBD.

10. Acknowledgments

The authors would like to thank Dino Farinacci, Michael Menth, Padma Pillay-Esnault, Alex Clemm, Uma Chunduri for their review and input on this document.

This document was produced using Marshall Rose's xml2rfc tool.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6115] Li, T., Ed., "Recommendation for a Routing Architecture", RFC 6115, DOI 10.17487/RFC6115, February 2011, <http://www.rfc-editor.org/info/rfc6115>.

[RFC6537] Ahrenholz, J., "Host Identity Protocol Distributed Hash Table Interface", RFC 6537, DOI 10.17487/RFC6537, February 2012, <http://www.rfc-editor.org/info/rfc6537>.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D., and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <http://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, <http://www.rfc-editor.org/info/rfc6833>.

[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, <http://www.rfc-editor.org/info/rfc6836>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <http://www.rfc-editor.org/info/rfc7401>.

[RFC7402] Jokela, P., Moskowitz, R., and J. Melen, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)", RFC 7402, DOI 10.17487/RFC7402, April 2015, <http://www.rfc-editor.org/info/rfc7402>.

[RFC8003] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Registration Extension", RFC 8003, DOI 10.17487/RFC8003, October 2016, <http://www.rfc-editor.org/info/rfc8003>.

[RFC8004] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 8004, DOI 10.17487/RFC8004, October 2016, <http://www.rfc-editor.org/info/rfc8004>.

[RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <http://www.rfc-editor.org/info/rfc8005>.

[RFC8046] Henderson, T., Ed., Vogt, C., and J. Arkko, "Host Mobility with the Host Identity Protocol", RFC 8046, DOI 10.17487/RFC8046, February 2017, <http://www.rfc-editor.org/info/rfc8046>.

[RFC8047] Henderson, T., Ed., Vogt, C., and J. Arkko, "Host Multihoming with the Host Identity Protocol", RFC 8047, DOI 10.17487/RFC8047, February 2017, <http://www.rfc-editor.org/info/rfc8047>.

[RFC8060] Farinacci, D., Meyer, D., and J. Snijders, "LISP Canonical Address Format (LCAF)", RFC 8060, DOI 10.17487/RFC8060, February 2017, <http://www.rfc-editor.org/info/rfc8060>.

[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, <http://www.rfc-editor.org/info/rfc8111>.

11.2. Informative References

[DNS-DUP] Yahya, B. and J. Ben-Othman, "Achieving host mobility using DNS dynamic updating protocol", October 2008, <http://ieeexplore.ieee.org/document/4664258/>.

[DNS1] Jung, J., Sit, E., Balakrishnan, H., and R. Morris, "DNS Performance and the Effectiveness of Caching", 2002, <http://nms.lcs.mit.edu/papers/dns-ton2002.ps>.

[DNS2] Liston, R., Srinivasan, S., and E. Zegura, "DNS Performance and the Effectiveness of Caching", 2002, <http://www.cc.gatech.edu/fac/Ellen.Zegura/papers/dnsdiversity.pdf>.

[DNS3] Briscoe, B., Anna Brunstrom, A., Andreas Petlund, A., David Hayes, D., David Ros, D., Ing-Jyh Tsang, I., Stein Gjessing, S., Gorry Fairhurst, G., Carsten Griwodz, C., and M. Michael Welzl, "Reducing Internet Latency: A Survey of Techniques and their Merits", November 2014, <http://ieeexplore.ieee.org/document/6967689/>.

[GNRS] Karimi, P. and S. Mukherjee, "Global Name Resolution Service", March 2017, <https://datatracker.ietf.org/doc/draft-karimi-ideas-gnrs/>.

[HHIT] Moskowitz, R., Xu, X., and B. Liu, "Hierarchical HITs for HIPv2", June 2017, <https://datatracker.ietf.org/doc/draft-moskowitz-hierarchical-hip/>.

[HIP-IP] Moskowitz, R., Xu, X., and B. Liu, "Encapsulation of IP within IP managed by HIP", June 2017, <https://datatracker.ietf.org/doc/draft-moskowitz-hip-IPnHIP/>.

[HIP-VPLS]
"HIP-based Virtual Private LAN Service (HIPLS)", February 2017, <https://datatracker.ietf.org/doc/draft-henderson-hip-vpls/>.

[IDEAS-IDY-USE]
"Identity Use Cases in IDEAS", June 2017, <https://datatracker.ietf.org/doc/draft-ccm-ideas-identity-use-cases/>.

[IDEAS-PS]
"Problem Statement for Identity Enabled Networks", March 2017, <https://datatracker.ietf.org/doc/draft-padma-ideas-problem/>.

[ILA] Herbert, T., "Identifier-Locator Addressing for Network Virtualization", March 2016, <https://datatracker.ietf.org/doc/draft-herbert-nvo3-ila/>.

[ILA-MS-TBD]
Herbert, T., "Re: [Ideas] A comment on the use case draft", March 2017, <https://www.ietf.org/mail-archive/web/ideas/current/msg00081.html>.

[IVIP] Whittle, R., "Ivip (Internet Vastly Improved Plumbing) Architecture", September 2010, <https://tools.ietf.org/html/draft-whittle-ivip-arch-04>.

[LISP-ANNOY]
"LISP EID Anonymity", April 2017, <https://datatracker.ietf.org/doc/draft-farinacci-lisp-eid-anonymity/>.

[LISP-DIS]
"LISP Discussion", <https://www.ietf.org/mail-archive/web/lisp/current/msg03733.html>.

[LISP-SEC]
Maino, F., Ermagan, V., Cabellos, A., Saucez, D., and O. Bonaventure, "LISP-Security (LISP-SEC)", Work in Progress, October 2012.

Authors' Addresses

Yingzhen Qu (editor)
Huawei
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: yingzhen.qu@huawei.com

Albert Cabellos
Technical University of Catalonia
C/ Jordi Girona s/n
Barcelona 08034
Spain

Email: acabello@ac.upc.edu

Robert Moskowitz
HTT Consulting
Oak Park, MI 48237
USA

Email: rgm@labs.htt-consult.com

Bingyang Liu
Huawei
156 Beiqing Rd
Beijing 100095
China

Email: liubingyang@huawei.com

Andreas Stockmayer
University of Tuebingen
room B305, Institute of Computer Science
Tuebingen 72076
Germany

Email: andreas.stockmayer@uni-tuebingen.de