Privacy Issues in Identifier Locator Separation Protocols

July, IETF 105

SAAG Meeting

Dirk von Hugo

Behcet Sarikaya

OUTLINE

- Identifier Locator Separation (idloc)
- Privacy Problem in IdLoc (pidloc)
- Use Cases
- Solution Space Analysis

Routing based on Id-Loc Separation

- End-to-end routing based on ‘traditional IP address approach’ may become inefficient and complex in case of e.g.
  - extreme mobility, multi-homing/multi-path, virtual vs. physical entities, …
- Identifier-Locator Separation (Id-Loc) may be advantageous here
- Multiple Protocols using Id-Loc proposed:
  - e.g. LISP (RFC 6833), ILNP (RFC 6740), ILA (draft-herbert-intarea-ila), …
- Several purposes:
  - reduce burden on IP(v6) address semantics, i.e. virtual machines
  - demand for new network architecture for seamless mobility, i.e. mapping system vs routing tables
  - Carry source-destination identifier instead of IP address in packet header
- Application areas include:
  - Industrial IoT
  - Vehicular Networks
  - 5G

ILA: Identifier Locator Addressing
ILNP: Identifier Locator Network Protocol
LISP: Locator/ID Separation Protocol

Routing based on Id-Loc Separation

- LISP (RFC 6833) as network-based approach
  - uses mapping and encapsulation of packets
  - proposes a specific LISP architecture providing a level of indirection for routing and addressing
  - specific ingress/egress routers at LISP domain boundaries
  - to obtain mappings used for encapsulation operation, routers query mapping system - only when necessary (e.g., at beginning of a new flow transmission)
  - Drafts rfc6830/6833-bis as proposed standards under IESG evaluation
    - https://www.lispers.net/ and https://datatracker.ietf.org/wg/lisp/

Routing based on Id-Loc Separation

- ILNP (RFC 6740) as host-based approach
  - 64 bit Locator is topologically significant and used only for routing and forwarding
  - 64 bit Node Identifier is not topologically significant and names a logical/virtual/physical node
  - enables mobility using mechanisms only deployed in end-systems not requiring any router changes
  - Uses DNS as mapping system
  - See also e.g. #102 tutorial
    - https://datatracker.ietf.org/meeting/102/materials/slides-102-edu-sessg-an-introduction-to-the-identifier-locator-network-protocol-ilnp-00
    - https://ilnp.cs.st-andrews.ac.uk/

Routing based on Id-Loc Separation

- ILA (draft-herbert-intarea-ila) using address transformation
  - proposes to split an IPv6 address identifier (lower address bits) and locator (higher address bits) portions à 64-bit length each
  - locator part determined dynamically from mapping table maintaining associations between 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.
  - A kernel implementation of ILA is available in Linux distribution.
  - ILA does not require any transport layer (UDP/TCP) changes.
  - See also #101 BoF ILA
    - https://datatracker.ietf.org/meeting/101/materials/slides-101-ila-ila-introduction-scope-and-isssues-03

Id-Loc Separation protocols - relation to security area

- Why privacy?
  - Source and destination identifiers at IP packet header as main issue for privacy
- What’s the threat?
  - Ids are carried in clear so exposure to 3rd parties to relate Ids to geo location
  - Multiple independent paths’ usage may increase location privacy attack risk
- What’s been tried in the past or now?
  - No solution yet but some proposed solutions like LISP CP, ILA FAST/AMS
- Why didn’t some of those get deployed/what are existing shortcomings?
  - Because Idloc protocols not yet deployed extensively
  - Privacy issue need to be addressed
  - A new architecture needs to be introduced
  - A more convenient mapping system is required
- What’s potential future work/pidloc ML/etc.?
  - BoF after developing Problem Statement and Requirements drafts from identified Use cases and subsequent WG formation to work on solution space

Privacy issues in ID/loc separation systems

- Check: https://tools.ietf.org/html/draft-nordmark-id-loc-privacy
  - Published just before IETF 102 in Montreal
- Pidloc non-WG discussion list was formed based on problems discussed in this draft right after IETF 102
- We have 60+ people on the list, we solicit more, please subscribe at https://www.ietf.org/mailman/listinfo/pidloc
- Some issues have been discussed in the past teleconferences and at least one solution draft has been submitted (Slide 11)

The Problem

- Location Privacy related to geographic location of device reachable at some IP address coupled identifier
- Movement Privacy derived from changing locator(s) of point of attachment at different times even without knowing particular locators and by possible correlation with other information (e.g., security cameras) to create a binding between identifier and personal device
- Strong privacy in address choice e.g. by creating frequently changing random values can present a scaling problem to the mapping in large networks

Use Cases

- **Optimized Routing** In an operator network the mapping system can provide access control so that only those trusted devices can access the mappings.
- **Business Assets** in Industrial IoT, share the ID/ locator binding within the company but not with 3rd parties
- **Distributed (cloud) Data center** in a restricted domain (walled garden) intruders may be prevented
- **Mobility and Global reach** in a cross-domain and -operator fashion would demand for explicit privacy preservation
- **NFV (Network Function Virtualization)** requires to find the optimum specific NF instance from a generalized NF name

Solution Space

- So far only one solution attempt https://tools.ietf.org/html/draft-herbert-route-fast-00
- Tom Herbert published this draft on Encoding Routing in Firewall and Service Tickets
- The architecture is adopted to 3GPP network
- Defines ILA locator encoding in a Firewall and Service Ticket (FAST) of 64 bits
- Locators of 128 bits like in LISP can also be defined

AMS draft

- Address Management System (https://tools.ietf.org/html/draft-herbert-intarea-ams-01) draft by Tom Herbert
- AMS routers have three primary functions:
  - Serving mapping information
  - Overlay forwarding
  - Sending redirects
- Proposes alternative to requiring a mapping lookup on each packet by encoding mapping information in specific FAST packets themselves
- Discusses interaction between address mapping system and privacy in Internet addressing in terms of criteria for and facilitation of strong privacy

LISP Control-Plane draft

- draft-ietf-lisp-rfc6833bis (Locator/ID Separation Protocol (LISP) Control-Plane) states that LISP Routers are not dependent on details of mapping database systems
- Can we think of applicability also to simplified approaches?

Next Steps

- In pidloc, we propose that before we find ways to protect privacy and avoid issues of location and movement privacy, first we need to work on a general Problem Statement and Requirements from identified Use cases
- Pidloc proposes exploring minimizing the privacy implication as a possible approach in Industrial IoT use case, i.e., one can explore limiting to which peers and when the ID/ locator binding are exposed
- Possible solutions like LISP CP and AMS/FAST should be adaptable to a generally applicable privacy preserving Id-Loc split protocol to be developed in the proposed WG and eventually apply to LISP, ILA, ILNP, and others.

Questions

- Subscribe to pidloc ML
  - https://www.ietf.org/mailman/listinfo/pidloc
- Review drafts
  - Requirements to Secure End to End Privacy in IdLoc Systems (draft-xyz-pidloc-reqs-00.txt)
  - Problem Statement for Secure End to End Privacy in IdLoc Systems (draft-xyz-pidloc-ps-02.txt)
- **Questions?**