Privacy Issues in Identifier Locator Separation Protocols pidloc

Chair Slides

March 27, IETF 104

pidloc side meeting

Dirk von Hugo

Behcet Sarikaya

Agenda

- Agenda bashing 5min (Dirk)
- State of the pidloc 15 min (Dirk)
- (p)id-loc in 5G 10 min (Shunsuke)
- Discussion 30 min
- Volunteers 5 min

Id-Loc Separation protocols

- Multiple Identifier-Locator Separation Protocols have been proposed (e.g. LISP, ILNP, ILA) in order to reduce burden on IP(v6) address semantics and demanding for new network architecture (providing high availability and agility through layer re-configuration and automation)
- Application areas include:
  - Industrial IoT (e.g. draft-irtf-t2trg-iot-seccons: State-of-the-Art and Challenges for the Internet of Things Security)
  - Vehicular Networks (see draft-kjsun-ipwave-id-loc-separation-00 which provides an architecture)
  - 5G (see draft-homma-dmm-5gs-id-loc-coexistence on low-impact Id-Loc Separation architecture for 3GPPs 5GSystem)

Privacy issues in ID/locator separation systems

- Draft (https://tools.ietf.org/html/draft-nordmark-id-loc-privacy) was 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 50+ 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 7)

The Problem

- Location Privacy related to geographic location of device reachable at some IP address coupled identifier and
- 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 in a cloud from a generalized NF name

Solution

- 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 (fast) ticket 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 Firewall and Service Ticket (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 CP 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/lightweight Id-Loc 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 as well as naming gaps in existing approaches
- Pidloc proposes exploring first minimizing the privacy implication, i.e., one can explore limiting to which peers and when the ID/ locator binding are exposed
- Possible solution space may cover AMS/FAST approach and LISP CP solutions and should be adaptable to a generally applicable privacy preserving Id-Loc split protocol (LISP, ILA, ILNP, etc.)