Privacy Issues in Identifier Locator Separation Protocols pidloc

Webex Call Slides

November/December 2018

Dirk von Hugo

Behcet Sarikaya

Agenda

- What was discussed so far
- Next Steps

draft-nordmark-id-loc-privacy

- Published just before IETF 102 in Montreal
- Pidloc non-WG discussion list was formed based on the problems discussed in this draft right after IETF 102
- We have app. 50 people on the list, we solicit more
- Some issues have been discussed and at least one solution draft has been submitted

The Problem

- Id-loc-privacy defines two problems:
- Location Privacy If a third party can at any time determine the IP location of some identifier, then the device can at one point be IP geolocated at home, and later a coffee shop
- Movement Privacy If a third party can determine that an identifier has changed locator(s) at time T, then even without knowing the particular locators before and after, it can correlate this movement event with other information (e.g., security cameras) to create a binding between the identifier and a person
- Id-loc privacy does not get into the issue of how to build a mapping system to protect the privacy and avoid the issues of location and movement privacy

The Work

- Id-loc-privacy instead proposes minimizing the privacy implication, i.e., one can explore limiting to which peers and when the ID/ locator binding are exposed
- 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.
- **Family and Friends** share location information with other family members or friends in IP level
- **Business Assets** in Industrial IoT, share the ID/ locator binding within the company but not share with 3rd parties

Discussion

- Family and Friends use case was questioned
- There are applications (life360) that use GPS location which is much more precise and convey it with secure connections
- Argument: it's a hard requirement that Identifiers (IP addresses in general) must not expose geo location of mobile devices, and it follows that identifier/locator bindings should never be shared outside a network except LEA orders

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
- Currently for ILA locators of 64 bit
- Locators of 128 bits like in LISP can also be used

Next Steps

- There is strong interest in the parties we talked (Ran Atkinson, Shunsuke Homma, Tom Herbert, etc.) on 5G as GTP-U replacement
- Should we go on this track?
- Another application is Industrial IoT with Edge Computing
- Erik Nordmark has a new draft on this which could be useful to discuss
- Any other areas of application of interest?