Privacy and network prefix assignment

draft-herbert-ipv6-prefix-address-privacy-00

Tom Herbert <tom@quantonium.net>

Caveats up front

- We only consider network layer (real privacy needs to be across all layers)
- We only consider risks to privacy by **third parties** making inferences
  - We do not consider privacy risks from information network providers will gather
  - We not consider jurisdictions where authorities can compel provider to provide PII

Prefix assignment

- /64 assignment to hosts is common
  - e.g by SLAAC
  - Assignment to UEs in mobile networks (RFC3314)
- Properties
  - Two addresses w/ same prefix refer to same device
  - 1-1 relationship between personal device and user
  - Prefix may contain fine grained hierarchy for routing

Privacy issue

- Prefix becomes an identifier of the device
- For personal device, prefix identifies user
- Risks exposing PII to third parties
  - User identity in communications
  - Location of users
- Issue is raised in RFC4941 and RFC7721
- Periodically changing IID (RFC4941) no help

Could prefix rotation work?

- Extrapolation of changing IIDs (RFC4941)
- Changing addresses is invasive
- What frequency of rotation ensures privacy?
- Quantitatively, anything less than different prefix per flow could be an issue
  - Postulated exploit to defeat prefix rotation

Criteria for privacy in addresses

- Given two addresses:
  - It can be inferred they belong to same organization
  - Possibly that they belong to same broad grouping
  - No other correlations can be made
    - Cannot infer that addresses refer to same node, user, department, etc.
    - Cannot infer accurate location or proximity
- NAT meets criteria with large enough pool!

Possible solution

- Identifier/locator split (such as ILA)
- Host are assigned “untrackable” addresses
- Addresses share common network prefix
- Meet criteria for strong privacy in addressing
- Maximum privacy: use a different source address for each flow

Practicality

- Address per flow is a lot of addresses!
  - Each address is entry in the mapping system
  - Singleton address assignment inefficient
- Potential mitigations
  - Not all communication require strong privacy
  - “Hidden aggregation”
    - Local network has secret means to map multiple addresses to an end node
    - Hidden aggregation block assignments to nodes using a form public key encryption

Thank you!