MIPv6 Privacy Extension
ALIEN BoF
63 IETF - Paris

Claude Castelluccia

Francis Dupont

Gabriel Montenegro

draft-dupont-mip6-privacyext-02

Problem

- MIPv6 data and signaling reveals
  - "identity" of the node (home address)
  - location of the node (care-of address)
- link between those two (who/where) revealed in
  - data (home address option and routing header option)
  - signaling (binding update)
- For unlinkability: avoid revealing binding between MN's HA and its CoA

Our proposal (1)

1. Change Interface IDs of care-of addresses across handoffs and per correspondent or group of correspondents (application of RFC 3041)

2. Generate a TMI (Temporary Mobile Identifier): a non-routable identifier (prefix to be assigned) per correspondent or group of correspondents

3. When the **communication is initiated by the mobile node** (Mobile Client case), it can choose to use the TMI instead.

   - but TMI is non-routable

   - so "route optimize" to use HoA Option and Routing Header

   - mobility without revealing its real HoA

Our proposal (2)

- Mobile Server case:
  - **Contact initiated by correspondent node** (via home agent)
  - If MN does bidirectional tunneling
    - does not reveal its CoA (location) to correspondent node
  - If MN does “route optimization”
    - TMI as “home address”
    - real home address in encrypted sub-option of binding updates (hidden to eavesdroppers)
    - subsequent data (HoA Option/routing header) uses TMI (eavesdroppers still get nothing)

TMI details

- Requirements:
  - Must follow the IPv6 address format
  - Must be unique per MN-CN pair
  - TMI ownership must be provable (to secure MIP6 signaling)
  - Mobile IPv6 signaling protection should be bound to TMIs (e.g., used as IPsec selectors)
  - TMIs must be identified as non routable
- Solution:
  - Use a (e.g., 8 or 16 bit) reserved prefix (to be assigned out of IPv6 addr space)
  - TMIs are Crypto-based Identifiers (CBIDs) like CGAs (Cryptographically Generated Addresses) or HIP HITs (Host Identity Payload - Host Identity Tags)

Conclusion

- Location privacy without a VPN and its cost
- Straightforward extensions from Mobile IPv6
- Combination with Hierarchical Mobile IPv6 allows finer tradeoffs
- Extensions for mobile server