Enabling Security/Privacy Addressing on 6LoWPAN Technologies

draft-thaler-6lo-privacy-addrs-00

Dave Thaler <dthaler@microsoft.com>

Privacy Considerations (RFC 6973 and draft-ietf-6man-ipv6-address-generation-privacy)

- Correlation of activities over time
  - If stable id used for Internet traffic across long period of time
- Location tracking
  - If stable id as move between different networks
- Address scanning
  - If stable id in IPv6 address narrows search space significantly
- Device-specific vulnerability exploitation
  - If id identifies vendor or version and hence suggests which attacks to try

- RFC 4941 and RFC 7217 solve these by:
  - Use pseudo-random (≥ 46 bits entropy) looking interface IDs that vary per network
  - Separate “temporary” address for privacy communication (e.g. outbound) from “stable” address for linkable communication (e.g. inbound)

Security considerations

- Some security schemes (CGA/HBA/etc) derive IPv6 addresses from keying material, e.g., to prevent spoofing
  - Usually requires 59 or more bits of entropy

6lowpan networks can be connected to the Internet, so same threats apply

So how can we mitigate without losing efficiency/etc.?

Let’s look at three potential approaches one could take:

1. Use of (random) IEEE-Identifier-Based Addresses
2. Use of 16-Bit Short Addresses
3. Use of Non-IEEE-Identifier-Based Addresses

1. Use of IEEE-Identifier-Based Addresses

- Can use per-network IEEE identifier with enough entropy to be roughly equivalent to RFC 7217
- Can use normal LOWPAN_IPHC encoding with stateless compression
- IPv6 addresses can be fully elided

- Mitigates privacy except for “Correlation of activities over time”
- Would need multiple uncorrelated addresses at times like:
  a) To separate privacy vs linkable-to-public-id communication
  b) Some overlap during a re-addressing event to avoid breaking connections
- Doesn’t help with the security (CGA/HBA/etc) uses

- Operational changes: minor

2. Use of 16-Bit Short Addresses

- Simple embedding lacks enough entropy to mitigate threats
- Could design a new address construction scheme though, e.g.
  - IPv6 IID = Hash64(L2 network key, short address)
- “Temporary” addresses could even be generated similarly, e.g.
  - IPv6 IID = Hash64(L2 network key, short address, ABRO version)
- Could use Context Identifier to distinguish between
  - non-temporary IPv6 IID
  - “current” temporary IPv6 IID
  - “past” temporary IPv6 IID
- Combination of the above could mitigate all the privacy threats mentioned, but would not support CGA/HBA
- Operational changes: moderate

3. Use of Non-IEEE-Identifier-Based Addresses

- All privacy/security items might be solvable if use stateful context-based compression that fully elides addresses
  - Also supports compressing DHCPv6 addrs even if don't care about privacy
  - Could also support compressing of addrs outside local network
  - Allows 16 arbitrary source addrs & 16 arbitrary dest addrs *per node*
- Context "prefix" is all 128 bits
- No change to base RFC 6775, but replaces substitutable context dissemination as used today
  - Context entry indexed by { **L2addr,** CID }
  - Each node generates/disseminates CIDs for its own addrs
    - Use 5 (of 24) reserved bits in ARO to send from host to router
    - Use 5 reserved bits in DAR/DAC to distribute between routers
  - Router's NCEs contain CID of neighbor's address
- Operational changes: LARGE

Example Sketch of #3