6lo Privacy Considerations

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

Dave Thaler <dthaler@microsoft.com>

Privacy Considerations for IPv6 Address Generation Mechanisms

draft-ietf-6man-ipv6-address-generation-privacy
(in IESG Evaluation) discusses four threats:

- 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
- Device-specific vulnerability exploitation
  - If id identifies vendor or version and hence suggests which attacks to try
- Address scanning
  - Non-random IPv6 interface id narrows search space significantly

Let’s look specifically at address scanning

- Address scans allow off-link attackers to discover a device to track/attack
- Thus enables all the other threats for off-link attackers
- Especially dangerous for any link that connects devices to the Internet or any other untrusted network
- To mitigate address scan, need about ~46 bits of entropy in IPv6 interface id for always-on devices
  - General rule is can address scan 2 addresses every second based on ICMP rate limit
  - Goal is to minimize chance of finding any device during lifetime of connection
  - # bits of entropy to get <50% chance ≈ log2(# devices) + log2(# scan tries) + 1
  - Example: 2^4 devices on a link lasting 2^5 seconds → need ~10 bits of entropy
- Ideally without losing efficiency/compression benefits in 6lowpan technologies

Let’s look at two potential approaches:

1. Random EUI-48 or EUI-64 addresses

2. “Short Addresses”

1. Random EUI-48 or EUI-64 addresses

- Can use per-network IEEE identifier with 46+ bits of entropy
- Can use normal LOWPAN_IPHC encoding with stateless compression
- IPv6 addresses can be fully elided

- Mitigates privacy threats except for “Correlation over time”
- Correlation over time can be mitigated if change EUI-48/64 often enough (e.g., each time you connect to a network)
  - See draft-huitema-6man-random-addresses and presentation in 6man
- Requires that L2 technology allows use of arbitrary EUI-48/EUI-64

Various Link Technologies

Technology	Reference	Bits of Entropy
802.15.4	RFC 4944	16+ or any EUI-64
Bluetooth LE	draft-ietf-6lo-btle-15	48
DECT ULE	draft-ietf-6lo-dect-ule-02	40 or any EUI-48
MS/TP	draft-ietf-6lo-6lobac-02	8 or 64
ITU-T G.9959	RFC 7428	8
NFC	draft-ietf-6lo-nfc-01	6 or ???
…		

2. Use of “Short Addresses” (e.g., 16-bit)

- Simple embedding lacks enough entropy to mitigate address scans unless link lifetime is extremely short
  - Padding with 0’s makes address scans easy
- Could use a different address construction scheme though, e.g.
  - IPv6 IID = Hash64(L2 network key, short address, ABRO version)
- Still allows full stateless compression/elision

Recommendations

- Security (privacy) sections should say how address scan is mitigated
  - Could be by forcing link to be very short lived
  - Could be by allow large number of bits of entropy
- Technologies must define a way to include sufficient bits of entropy in the interface id based on the maximum link lifetimes
  - Random EUI-48/EUI-64 is one easy way to do so for some link technologies
- Do not simply use a short address padded with a well-known prefix unless link lifetime is guaranteed to be extremely short
- Make sure that an IPv6 address can change over long period of time
  - E.g. each time it connects to the network, or each day, or whatever
  - This mitigates correlation over time
- If a device can roam between networks AND more than a few bits of entropy exist in the IPv6 iid, then make sure it can vary per network
  - This mitigates location tracking