Observations on IPv6 Addressing

(draft-struik-6lo-on-ipv6-addressing-00)

—

René Struik
E-mail: rstruik.ext@gmail.com
Outline

1. IPv6 Addressing
   − Problems with IPv6 Addressing using Modified EUI-64 Addresses
   − Opaque Interface Identifiers (RFC 7217) to the Rescue
   − Does this address stated privacy and security issues?
   − Layering aspects
   − What about susceptibility to Big Brother-esque subliminal channels?

2. Subliminal channels in Big-Brother-esque world
IPv6 Addressing Using Modified EUI-64 Hardware Addresses

Issues:
- *Fixed IID* over time.
  Correlation of activities over time.
- *Fixed IID* across networks.
  Tracking/correlation across different networks.
- *Encoding of device characteristics via IID*.
  Leakage of device properties (including potential device-specific shortcomings).
- *Device-specific addresses*.
  Device replacement causes change of IPv6 address.

**Suggested remedy (RFC 7217):** semantically opaque IID (RIDs).

Random IID (RID) = $F$(*secret device key, public parameters*), where
- $F$ hard to invert;
- $F$ difficult to compute without *secret key*;
- Output size $F$ at least 64 bits.
- *Public parameters* = \{*Prefix, Net_Iface, Network Id*\}
IPv6 Addressing Using Opaque IIDs to the Rescue?

How this addresses identified issues:

- **Fixed IID over time. Not addressed**
  Still tracking/correlation within same network (both temporal and spatial).

- **Fixed IID across networks. Addressed**
  No tracking/correlation across different networks.

- **Encoding of device characteristics via IID. Addressed**
  No logical dependency between EUI-64 hardware address and opaque ID
  
  NOTE1: Also realized by deriving IID from randomly generated MAC address.
  NOTE2: Compression benefits, which are also realized other way around (i.e., if MAC address derived from opaque IID)

- **Device-specific addresses. Addressed**
  However, this does require cloning of secret device key to replacement device).
  NOTE: Not clear whether “device cloning” would be desirable at all (since presenting a security event – and new device is logically different security entity)
Layering Aspects of Addressing (1)

- Application
- Transport
- Data Link
- Physical

Device A

“Tunnel” Device

Router

Device B

Layering diagram showing the interaction between different network layers.

Per-hop traceability if MAC addresses ‘fixed’, no matter whether IPv6 IIDss randomized or not.
No address traceability if MAC addresses ‘random’ and IPv6 IID’s randomized (or one derived from other)
Layering Aspects of Addressing (3)

Layer address traceability undoes effect of Layer 3 address randomization (on per-hop level)

Potentially better approaches than opaque IIDs:
1. Derive IID from randomly generated MAC address;
2. Derive MAC address from random IID (that does not have any of remaining caveats Opaque IIDs)
Random IID (RID) = $F(\text{secret device key}, \text{public parameters})$, where

- $F$ hard to invert;
- $F$ difficult to compute without secret key;
- Output size $F$ at least 64 bits.
- Public parameters = \{Prefix, Net_IFace, Network Id\}

Administrator access to secret device key (for device cloning) presents potential security vulnerability.

Opaque interface identifier serves as subliminal channel for leakage of keying material:

- Proper implementation of $F$ cannot be detected without close examination of entire device implementation
- $F$ could have been implemented so as to leak 64 bits (or more) of device-internal information, e.g., by setting $F:=E_{KM}(k) \pmod{2^{64}}$, where $k$ is device-internal secret (seed random number generator, private key, etc.) and where $KM$ is key escrow key

NOTE: This is based on concepts CRYPTO 2014 paper [9]; some details omitted
Note on Susceptibility of Address Randomization (2)

How to detect subliminal channels in generation of opaque-style interface identifiers?

If generated with

- *symmetric keys:*
  Not possible to detect without close scrutiny entire device implementation

- *public keys:*
  Might be possible to detect via variant of Cryptographically Generated Addresses (RFC 3972)
  NOTE: here, larger-size IIDs (i.e., more than 64 bits [7]) help.
Conclusions & Recommendations

- It is not clear how useful RFC 7217 is in addressing privacy issues
- Any approach ignoring Layer 2 traceability aspects mostly undoes benefits
- Not necessary to logically untie Layer 2 and Layer 3 addressing, if chosen with care (thus, allowing compression using cross-layer info)
- Beware of subliminal channels…
- Subliminal channels may be thwarted by using cryptographically generated addresses (CGAs) that can be verified. This requires more work
Further Reading


3. RFC 6282, ‘Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks,’ September 2011.


5. RFC 6775, Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LowPANs), November 2012.


