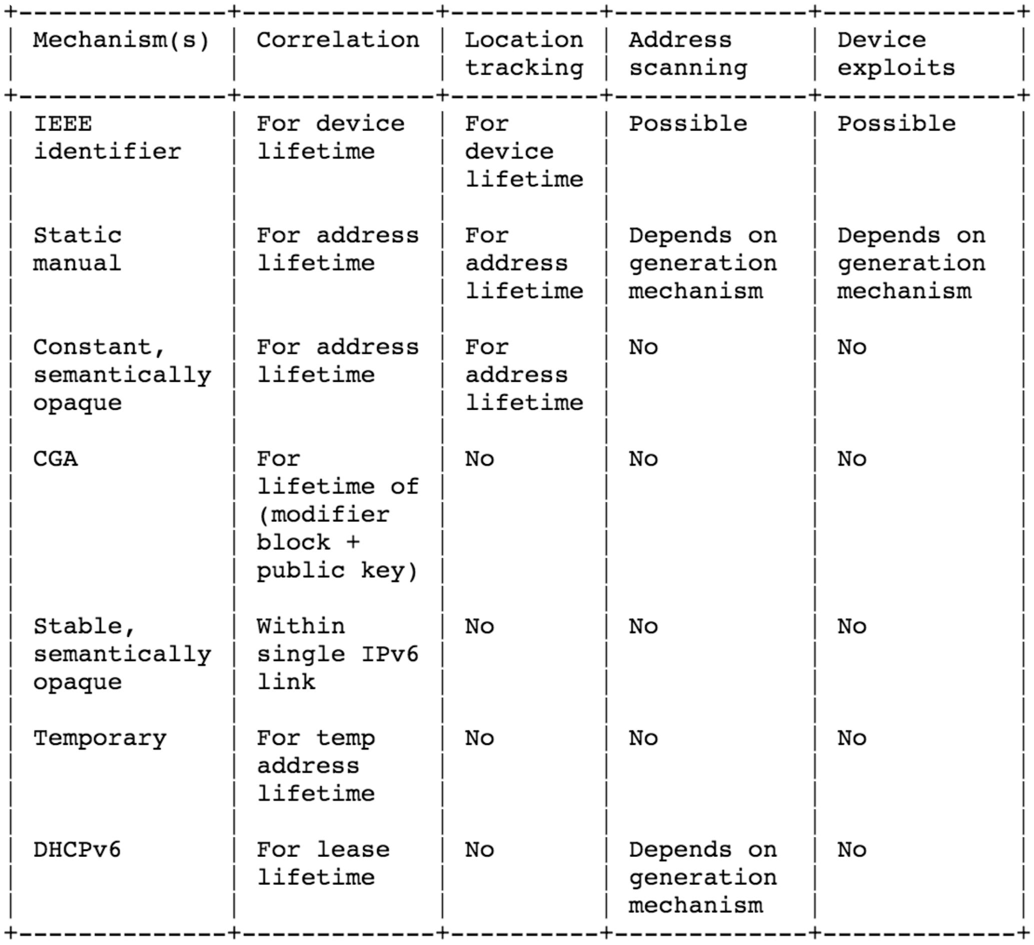
draft-ietf-6man-default-iids

Work motivated by …

RFC 7721



Mechanism(s)	Correlation	Location tracking	Address scanning	Device exploits
IEEE identifier	For device lifetime	For device lifetime	Possible	Possible
Static manual	For address lifetime	For address lifetime	Depends on generation mechanism	Depends on generation mechanism
Constant, semantically opaque	For address lifetime	For address lifetime	No	No
CGA	For lifetime of (modifier block + public key)	No	No	No
Stable, semantically opaque	Within single IPv6 link	No	No	No
Temporary	For temp address lifetime	No	No	No
DHCPv6	For lease lifetime	No	Depends on generation mechanism	No

RFC 7217

RID = F(Prefix, Net_Iface, Network_ID, DAD_Counter, secret_key)

Stable addresses

- IPv6 nodes employing SLAAC configure at least one stable address
    - Temporary addresses configured along with them

- All IPv6-over-foo specs require that, when generating such stable addresses, a link-layer ID (such as MAC address) be embedded in the IPv6 IID

- draft-ietf-6man-default-iids updates all IPv6-over-foo documents such that the default algorithm for generating stable addresses is RFC7217

draft-ietf-6man-default-iids-09 (1/2)

Link layers MUST define a mechanism that provides mitigation of the security and privacy implications discussed in Section 1. Such mechanism MUST meet the following requirements:

1. IID stable per prefix used with SLAAC within each subnet for same network interface
2. IID must change when prefix changes
3. IID must be difficult for outsider to predict
4. IID must be semantically opaque

Nodes SHOULD implement and employ [RFC7217] as the default scheme for generating stable IPv6 addresses with SLAAC.

draft-ietf-6man-default-iids-09 (2/2)

By default, nodes SHOULD NOT employ IPv6 address generation schemes that embed the underlying hardware address in the Interface Identifier.

Nodes SHOULD NOT generate Interface Identifiers with the schemes specified in [RFC2464], [RFC2467], [RFC2470], [RFC2491], [RFC2492], [RFC2497], [RFC2590], [RFC3146], [RFC3572], [RFC4338], [RFC4391], [RFC4944], [RFC5121], and [RFC5072].

…

Summary of recent list discussion (1/2)

- Comments about focus being limited to stable addresses only
  - Claim that context needs to be clarified: RFC 4941 orthogonal, where MAC address not randomized, and stability is desirable
  - Need to avoid foreclosing “temporary-only” case?
    - Temporary-only implies RFC 4941 update

Summary of recent list discussion (2/2)

- Interaction with MAC address randomization

  - Claim that requiring 7217 undercuts privacy/security benefits of MAC address randomization
    - But discussion of case where randomized MAC address used as Net_Iface parameter of RFC7217

  - Discussion of drawbacks of embedding MAC address in IID
    - IPv6 implementations not in control of MAC address generation method
    - Cases where random MAC address not allowed or algorithm not appropriate
    - Other downsides – wasted entropy, interop

Decisions, decisions

1. Maintain and clarify stable scope? Or something else?

2. Recommend specific mechanisms, or just state requirements?
   - If specific mechanisms and broader scope, what if we don’t have standards for every case?
   - If just requirements, what happens to IP-over-foo document updates?

3. Assume link layer address is opaque to address generation mechanism or craft exception cases where MAC address is randomized?