draft-ietf-6man-ipv6-address-generation-privacy-01

Alissa Cooper
Fernando Gont
Dave Thaler

Updates in -01

- Link-locals out of scope
  - Unique-locals out of scope (to add in -02)
- Refined analysis in Section 4 for CGAs and DHCPv6
- Corrected errors in Section 4 summary table
- Editorial fixes

CGAs

- Modifier block changes per IID generated, so correlation can last for lifetime of (modifier block + public key).
- Subnet prefix is input to hash function, so location tracking is not possible.

DHCPv6

- Recent releases of most popular DHCPv6 server software typically lease random addresses with a similar lease time as that of IPv4
  - Same properties as stable, semantically opaque IIDs.
- Some DHCPv6 software leases sequential addresses (typically low-byte addresses), which allow address scans.

Privacy and security properties

Mechanism	Correlation	Location tracking	Address scanning	Device exploits
IEEE identifier	For device lifetime	For device lifetime	Possible	Possible
Static manual	For address lifetime	~~Depends on generation mechanism~~ For address lifetime	Depends on generation mechanism	Depends on generation mechanism
Constant, semantically opaque	~~For OS lifetime~~ For address lifetime	~~For OS lifetime~~ For address lifetime	No	No

Privacy and security properties cont'd

Mechanism	Correlation	Location tracking	Address scanning	Device exploits
CGA	~~For public key lifetime~~ For lifetime of (public key + modifier block)	~~For public key lifetime~~ No	No	No
DHCPv6	For lease lifetime ~~(typically hours)~~	No	~~Depends on DHCPv6 server implementation~~ Depends on generation mechanism	No

Privacy and security properties cont'd

Mechanism	Correlation	Location tracking	Address scanning	Device exploits
Stable, semantically opaque	~~Possible for OS lifetime~~ Within single network	No	No	No
Temporary	For temporary address lifetime	No	No	No

Next steps

- WGLC?