A Method for Generating Semantically Opaque IPv6 Interface Identifiers (IIDs) with DHCPv6

(draft-gont-dhcwg-dhcpv6-iids-00)

F. Gont, SI6 Networks

dhc WG. IETF 122
Bangkok, Thailand. March 14th-21st, 2025

Motivation

- RFC 9416 / BCP 72 (“Security Considerations for Transient Numeric Identifiers Employed in Network Protocols”):

> **Protocol specifications that employ transient numeric identifiers SHOULD recommend an algorithm for generating the aforementioned transient numeric identifiers that mitigates the vulnerabilities identified in the previous step, such as those discussed in [RFC9415].**

- draft-ietf-dhc-rfc8415bis contains a non-RFC2119 reference to RFC 7610
- Future revisions of the DHCPv6 spec would benefit from a Std Track version of the mechanism (comply with RFC 9416, without a downref).

draft-gont-dhcwg-dhcpv6-iids-00

- Std Track version of RFC 7610 (Informational)
- Proposes an algorithm to select IPv6 IIDs that:
  - Do not result in address patterns
  - Are different for each network prefix
  - Are stable for each client
  - Will result in the same IIDs even without storing the leases
- It is a DHCPv6-version of the algorithm in RFC 7217, employed with SLAAC

Algorithm: RID computation

`RID = F(Prefix | Client_DUID | IAID | Counter | secret_key)`

Where:

- RID: Randomized identifier (will be the basis for the leased address)
- F(): Hash function (we recommend SHA-256)
- Prefix: IPv6 prefix employed for the address pool (unused bits set to 0)
- Client_DUID: DUID contained in the received Client Identifier Option
- IAID: IAID contained in the received IA_NA option
- Counter: Counter value that is employed to resolve address conflicts
- secret_key: Secret key (unknown to the attacker)

Algorithm: Steps

1) Compute RID
2) Select candidate address as:

```
IPV6_ADDR = IPV6_ADDR_LOW +
            RID % (IPV6_ADDR_HI - IPV6_ADDR_LOW + 1)
```

3) Compare IPv6 IID to reserved IIDs: if unacceptable, increment **`Counter`** and redo (go back to step #1)
4) If the address is unavailable or marked as “declined”, increment **`Counter`** and redo (go back to step #1)
5) Use the computed address

Next steps

- Comments/questions?
- Adopt as WG document?