CGA SEC Option for Secure Neighbor Discovery (SeND) Protocol

draft-jiang-6man-cga-sec-option

IETF 91 6man WG

November, 2014

Sheng JIANG
Dacheng ZHANG (Speaker)

Background & Motivation

- Cryptographically Generated Addresses (CGA) has been defined by RFC3972, 2005
- SEC bits, an important parameter in the generation of CGAs, are used to artificially introduce additional difficulty in order to provide additional protection against brute force attacks.
- However, the SeND protocol fails to distribute the SEC values to the hosts. As a result, the network administration cannot propagate any requirements regarding to SEC value of host-generated CGA addresses. It is actually a barrier for CGA and SeND to be widely used.
- In order to fill this gap, this document introduces a new CGA SEC Option.

CGA SEC Option

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     OPTION_CGA_SEC_OPTION     |       option-len              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    SEC bits   |
+-+-+-+-+-+-+-+-+
```

Host Behavior

- On receiving the CGA SEC Option with a recommended SEC value, a host SHOULD use a CGA with the recommended or higher SEC value. If choosing a CGA with a SEC value lower than the recommended, the host MAY take the risk that it is not able to use full network capabilities. The network may consider the hosts that use CGAs with lower SEC values as unsecure users and decline some or all network services.

Next step: WG adoption?

Comments are welcomed!

Thank You!