Configuring Cryptographically Generated Addresses (CGA) using DHCPv6

draft-jiang-dhc-cga-config
IETF 77, DHC WG
March 25, 2010

Sheng Jiang (Speaker)
Sam Zhongqi Xia
• DHCPv6 can be extended to:
  propagate to the parameters that a host needs to generate a CGA

– **Parameters needed for the generation of CGA**
  ✓ Prefix (RA or draft-xia-dhc-host-gen-id)
  ✓ Sec value (new DHCPv6 option in this draft)
  ✓ A Key Pair (Pre-configured or self generated)
  ✓ Extension Fields (not have user case currently)
Requirements & Motivation (2)

• CGA generation can computational consumption
  Proposed new interaction: a host may send a request to ask a DHCPv6 server to help computing a CGA for it

• Test Results of CGA Generating Time
  • Platform
    – An Intel Due 2 (2.53GHz) workstation
    – An laboratory implementation of CGA & SEND
  • Results of average CGA generating time
    – SEC=0: 100 µs
    – SEC=1: 60 ms
    – SEC=2: 2000s (varies from 100~7000sec)
    – SEC=3: N/A (theoretically estimating, more than 30,000 hours are required
  • Each SEC level, computational consumption is increased by $2^{16}$
**DHCPv6 Approach (CGA parameter configuration)**

- A node initiates a request for the relevant CGA configuration information to the DHCPv6 server
  - The Option Request Option [RFC3315] can be re-used
- DHCPv6 server responses the requested CGA-related parameters
  - Prefix, draft-xia-dhc-host-gen-id defined a new Identity Association for Prefix Assignment Option
  - SEC value, a new CGA-Sec Option is defined
DHCPv6 Approach (CGA computation offloading)

- A node may initiate a request for the computation of a CGA to the DHCPv6 server
  - a new CGA Generation Request Option is defined

- DHCPv6 server MAY use IA_NA or IA_TA option to return the CGA address and associated CGA Parameters data structure
Comments are welcomed!

Thank You!

Sheng Jiang (shengjiang@huawei.com)
Sam (Zhongqi) Xia (xiazhongqi@huawei.com)