draft-van-beijnum-cga-dhcp-interaction-00.txt

IETF 70, December 2007, Vancouver

Iljitsch van Beijnum

What

- Possible use of DHCPv6 to configure CGA parameters
- Parameters:
    - Sec
    - Public key
    - Subnet prefix

Sec

- Sec determines strength of crypto address
- Must be high enough → no bidding down
- But: too high → effectively a DoS attack
- And: depends on administrative host config or local network?
- DHCPv6 may not be appropriate for Sec
    - except maybe with DHCPv6 auth option

Public key

- Ability to manage public/private key pair central to CGA operation
- External configuration doesn't seem useful
  - except if CGA is done on proxy
  - in that case: DHCPv6 address assignment

Subnet

- CGA is generated for a specific subnet
- DHCPv6 servers can't supply subnet
  - maybe add this capability?
  - (and/or let DHCPv6 server assign IID)
  - how does DHCPv6 server know the CGA host's subnet, anyway?

Modifier???

- Is configuring a modifier useful?

Sec offloading

- Creating CGA with Sec > 0 cost a lot of CPU
- Slow/battery powered devices may want to offload this
- No sensitive information involved
- In that case, need to configure address of crypto processing server (DHCPv6...?)

Proxy CGA

- Checking: no changes needed, let proxy check and drop if unsuccesful
- Challenges: would need secure channel to proxy...
  - MCGAs could be useful
    - see MCGA document

Address registration

- Enterprise admins (and ISPs?) want to know which host has which IPv6 address
- Having address assigned by DHCPv6 server incompatible with CGA
- But could list generated CGA in IA option, server registers rather than assigns address
  - no protocol change, maybe implementation change

Certificate provisioning

- To use CGA, need to know trustworthiness of certificates
- Could learn through DHCPv6
    - but need secure DHCPv6 operation → DHCPv6 authentication option
    - just exchange fingerprints?
        - message size issue, modest security anyway

DHCPv6 work

- Subnet option in DHCPv6?
- Crypto offload server option?
- Option for certificate trustworthiness?

- Start using IA option for address registration

Questions?

- draft-van-beijnum-cga-dhcp-interaction-00.txt