Network Working Group   Sheng Jiang
Internet Draft   Sam(Zhongqi) Xia
Intended status: Standards Track   Huawei Technologies Co., Ltd
Expires: May 06, 2013   November 05, 2012

Configuring Cryptographically Generated Addresses (CGA) using DHCPv6
draft-ietf-dhc-cga-config-dhcpv6-04

Status of this Memo

Copyright Notice

Abstract

A Cryptographically Generated Address is an IPv6 addresses binding with a public/private key pair. However, the current CGA specifications are lack of procedures to enable proper management of the usage of CGAs. This document analyzes the parameters required for the generation of CGA from network configuration and management perspective. The configuration procedures of many CGA-relevant parameters with existing mechanisms are described in the document. Only Sec value has no suitable mechanism to be configured by network admin. A new DHCPv6 option is defined accordingly. This document also analyses the configuration of the parameters, which are used to generate CGAs, using DHCPv6. Although the document does not define new DHCPv6 option to carry these parameters for various reasons, the configuration procedure is described.

Table of Contents

1. Introduction

Cryptographically Generated Addresses (CGA, [RFC3972]) provide means to verify the ownership of IPv6 addresses without requiring any security infrastructure such as a certification authority.

CGAs were originally designed for SeND [RFC3971] and SeND is generally not used in the same environment as a Dynamic Host Configure Protocol for IPv6 (DHCPv6) [RFC3315] server. However, after CGA has been defined, as an independent security property, many other CGA usages have been proposed and defined, such as Site Multihoming by IPv6 Intermediation (SHIM6) [RFC5533], Enhanced Route Optimization for Mobile IPv6 [RFC4866], also using the CGA for DHCP security purpose [I-D.ietf-dhc-secure-dhcpv6], etc. The use of CGAs allows identity verification in different protocols. In these scenarios, CGAs may be used in DHCPv6-managed networks.

This document analyses the configuration of the parameters, which are used to generate CGAs, from network configuration and management perspective. Although the document does not define new DHCPv6 option to carry these parameters for various reasons, the configuration procedure is described. The procedure works with existing options or future define options.

In current specifications, the network administration can NOT grant the use of host-generated CGA addresses on request from the client, or reject the CGA on the basis of a too-low sec value. In order to fill this gap, a new DHCPv6 option, CGA Grant Option, is defined in this document.

The CGA configuration procedure described in this document can work with a generic address registration mechanism. However, even a generic address registration mechanism was defined, the CGA-specific option, CGA Grant Option, is still needed so that DHCPv6 server can indicate hosts the recommended CGA Sec value.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

3. CGA Configure Process Using DHCPv6

The CGA specifications [RFC3972] define the procedure to generate a CGA. However, it assumes that hosts decide by itself or have been preconfigured all CGA relevant parameters. In reality, the network management MAY want to assign/enforcement some parameters to hosts; the network management MAY also manage the use of CGAs.

Among the mechanisms in which configuration parameters could be pushed to the end hosts and/or CGA related information sent back to a central administration, we discuss the stateful configuration mechanism based on DCHPv6 in this document. Other mechanisms may also provide similar functions, but out of scope.

In this section, configuration CGA parameters and that a DHCPv6 server grants the CGA usage are described in details.

3.1. Configuration of the parameters required for the generation of CGA

Each CGA is associated with a CGA Parameters data structure, which is formed by all input parameters [RFC3972] except for Sec value that is embedded in the CGA. The CGA associated Parameters used to generate a CGA includes:

- a Public Key,

- a Subnet Prefix,

- a 3-bit security parameter, Sec. Additionally, it should be noted that the hash algorithm to be used in the generation of the CGA is also defined by the Sec value [RFC4982],

- any Extension Fields that could be used.

- Note: the modifier and the Collision Count value in the CGA Parameter data structure are generated during the CGA generation process. They do NOT need to be configured.

In a DHCPv6 managed network, a host may initiate a request for the relevant CGA configuration information needed to the DHCPv6 server. The server responds with the configuration information for the host. The Option Request Option, defined in Section 22.7 in [RFC3315], can be used for host to indicate which options the client requests from the server. For response, the requested Option should be included. The server MAY also initiatively push these parameters by attaching these option in the response messages which are initiated for other purposes.

- The Public/Private key pair is generated by hosts themselves and considered not suitable for network transmission for security reasons. The configuration of the client key pair or certificate is out of scope.

- Currently, there are convenient mechanisms for allowing an administrator to configure the subnet prefix for a host, by Router Advertisement [RFC4861, RFC4862]. However, this does not suitable for the DHCP-managed network. To propagate the prefix through DHCP interactions, DHCPv6 Prefix Delegation Option [RFC3633] MAY be used. However, this option was designed to assign prefix block for routers. A new Prefix Assignment Option MAY need to be defined. Since alternative approach is existing and there are debates whether a new Prefix Assignment Option MAY is necessary, this document does not define it.

- Although the network management MAY want to enforce or configure a Sec value to the hosts, it is considered as a very dangerous action. A malicious fake server may send out a high Sec value to attack clients giving the fact that generation a CGA with a high Sec value is very computational intensive. Another risk is that a malicious server could propagate a Sec value providing less protection than intended by the network administrator, facilitating a brute force attack against the hash, or the selection of the weakest hash algorithm available for CGA definition. A recommendation Sec value is considered as confusion information. The receiving host is lack for information to make choose whether generates a CGA according to the recommendation or not. Therefore, the document does not define a DHCPv6 option to propagate the Sec value.

- Although there is an optional Extension Fields in CGA Parameter data structure, there is NO any defined extension fields. If in the future, new Extension Fields in CGA Parameter data structure are defined, future specification may define correspondent DHCPv6 options to carry these parameters.

Upon reception of the CGA relevant parameters from DHCPv6 server, the end hosts SHOULD generate addresses compliant with the received parameters. If the parameters change, the end hosts SHOULD generate new addresses compliant with the parameters propagated.

3.2. Host requests CGA Approved to the DHCPv6 server

A CGA address is generated by the associated key pair owner, normally an end host. However, in a DHCPv6-managed network, hosts should use IPv6 global addresses only from a DHCPv6 server. The process

described below allows a host, also DHCPv6 client, uses self-generated CGAs in a DHCPv6-managed environment, by requesting the granting from a DHCPv6 server.

The client sends a CGA, which is generated by itself, to a DHCPv6 server, and requests the DHCP server to determine whether the generated CGA satisfies the requirements of the network configuration, wherein the network configuration comprises a CGA security level set by the DHCP; and generates a new CGA if the generated CGA does not satisfy the requirements of the network configuration.

- Client initiation behavior

  In details, a DHCPv6 client SHOULD send a DHCPv6 Request message to initiate the CGA granting process.

  This DHCPv6 Request message MUST include an Option Request option [RFC3315], which requests the CGA Grant Option, defined in Section 4 in this document, to indicate the DHCPv6 server responses with the address granting decision.

  The client MUST include one or more IA Options, either IA_NA or IA_TA, in the Request message. Each IA Option MUST includes one or more IA Address Options. CGAs are carried in the IA Address Options.

- Server behavior

  Upon reception of the Request message, the DHCPv6 server SHOULD verify whether the client's CGAs satisfy the CGA-related configuration parameters of the network. The DHCPv6 server then send an acknowledgement, a Reply message, to the client to either grant the use of the CGA or decline the requested CGA. The CGA_Grant field SHOULD be set following the rule, defined in Section 4 in this document. When the requested CGA is declined, the DHCPv6 server MAY also recommend a Sec value to the client using the CGA Grant option in the DHCPv6 Reply message.

  In the meantime, the DHCPv6 server MAY log the requested CGA addresses. This information MAY later be used by other network functions, such as ACL.

- Client receiving behavior

  Upon reception of the acknowledgement from server, the client can legally use the granted CGAs. The client SHOULD silently drop any

message that has the CGA_Grant field set any other value, but F0x, or 00x~07x. If the server declines the requested CGA, the client MAY generate a new CGA with the recommended Sec value. If the server replies with CGA-relevant parameters, the client MAY generate a new CGA accordingly.

4. CGA Grant Option

DHCPv6 CGA Grant Option is used to indicate the DHCPv6 client whether the requested address is granted or not. In the decline case, a recommended Sec value MAY be sent, too.

```
 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_ADDR_GRANT       |       option-len              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   CGA Grant   |
+-+-+-+-+-+-+-+-+
```

option-code

OPTION_ADDR_GRANT (TBA1).

option-len

1.

CGA_Grant

In the DHCPv6 reply message, the CGA_Grant field sets F0x to indicate that the requested CGA is granted; it sets 00x to indicate that the requested Address is declined without any recommended Sec value. It sets 01x~07x to indicate that requested Address is declined and the recommended Sec value (value from 1~7).

Note: On receiving the CGA Grant Option with reject information and a recommended Sec value, the client MAY generate a new CGA with the recommended Sec value. If choosing not use the recommended Sec value, the client 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.

5. Security Considerations

The mechanisms based on DHCPv6 are all vulnerable to attacks to the DHCP client. Proper use of DHCPv6 autoconfiguration facilities [RFC3315], such as AUTH option or Secure DHCP [I-D.ietf-dhc-secure-dhcpv6] can prevent these threats, provided that a configuration token is known to both the client and the server.

IF a DHCPv6 server rejected a client CGA based on a certain Sec value, it SHOULD NOT suggest a new Sec value either equal or lower than the Sec value that has been rejected.

Note that, as expected, it is not possible to provide secure configuration of CGA without a previous configuration of security information at the client (either a trust anchor, or a DHCPv6 configuration token, etc.). However, considering that the values of these elements could be shared by the hosts in the network segment, these security elements can be configured more easily in the end hosts than its addresses.

6. IANA Considerations

This document defines two new DHCPv6 [RFC3315] options, which must be assigned Option Type values within the option numbering space for DHCPv6 messages:

The DHCPv6 CGA Grant Option, OPTION_ADDR_GRANT (TBA1), described in Section 4.

7. Acknowledgments

The authors would like to thank Marcelo Bagnulo Braun and Alberto Garcia-Martinez for been involved in the early requirement identification. Valuable comments from Bernie Volz, Ted Lemon, John Jason Brzozowski, Dujuan Gu and other DHC WG members are appreciated.

8. References

8.1. Normative References

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC2119, March 1997.

[RFC3315] R. Droms, Ed., "Dynamic Host Configure Protocol for IPv6", RFC3315, July 2003.

[RFC3633] O. Troan and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC3971] J. Arkko, J. Kempf, B. Zill and P. Nikander, "SEcure Neighbor Discovery (SEND) ", RFC 3971, March 2005.

[RFC3972] T. Aura, "Cryptographically Generated Address", RFC3972, March 2005.

[RFC4861] T. Narten, et al., "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] S. Thomson, T. Narten and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC4862, September 2007.

[RFC4866] J. Arkko, C. Vogt and W. Haddad, "Enhanced Route Optimization for Mobile IPv6", RFC4866, May 2007.

[RFC4982] M. Bagnulo, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs) ", RFC4982, July 2007.

[RFC5533] E. Nordmark and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6" FRC 5533, June 2009.

8.2. Informative References

[I-D.ietf-dhc-secure-dhcpv6]
S. Jiang and S. Shen, "Secure DHCPv6 Using CGAs", draft-ietf-dhc-secure-dhcpv6 (work in progress), Septerber, 2012.

Author's Addresses

Sheng Jiang
Huawei Technologies Co., Ltd
Q14 Huawei Campus, 156 BeiQi Road,
ZhongGuan Cun, Hai-Dian District, Beijing 100085
P.R. China
Email: jiangsheng@huawei.com

Sam(Zhongqi) Xia
Huawei Technologies Co., Ltd
Q14 Huawei Campus, 156 BeiQi Road,
ZhongGuan Cun, Hai-Dian District, Beijing 100085
P.R. China
Email: xiazhongqi@huawei.com