Network Working Group
Internet Draft
Intended status: Informational
Expires: June 18, 2010

Sheng Jiang
Huawei Technologies Co., Ltd
Sean Shen
CNNIC
Tim Chown
University of Southampton

December 16, 2009

# DHCPv6 and CGA Interaction: Problem Statement

draft-ietf-csi-dhcpv6-cga-ps-01.txt

## Status of this Memo



## Copyright Notice

Abstract

This document describes potential issues in the interaction between DHCPv6 and Cryptographically Generated Addresses (CGAs). Firstly, the scenario of using CGAs in DHCPv6 environments is discussed. Some operations are clarified for the interaction of DHCPv6 servers and CGA-associated hosts. We then also discuss how CGAs and DHCPv6 may have mutual benefits for each other, including using CGAs in DHCPv6 operations to enhance its security features and using DHCPv6 to provide the CGA generation function.

Table of Contents

## 1. Introduction

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [RFC3315] can assign addresses statefully. Although there are other ways to assign IPv6 addresses [RFC4862, RFC4339], DHCPv6 is still useful when an administrator requires more control over address assignments to hosts. DHCPv6 can also be used to distribute other network configuration information.

Cryptographically Generated Addresses (CGAs) [RFC3972] are IPv6 addresses for which the interface identifiers are generated by computing a cryptographic one-way hash function from a public key and auxiliary parameters. By using the associated public & private keys as described by SEcure Neighbor Discovery (SEND) [RFC3971], CGAs can protect the Neighbor Discovery Protocol (NDP) [RFC4861], i.e. they can provide address validation and integrity protection for NDP messages.

This document describes potential issues in the interaction between DHCPv6 and Cryptographically Generated Addresses (CGAs). Firstly, the scenario of using CGAs in DHCPv6 environments is discussed. Some operations are clarified for the interaction of DHCPv6 servers and CGA-associated hosts. We then also discuss how CGAs and DHCPv6 may have mutual benefits for each other, including using CGAs in DHCPv6 operations to enhance its security features and using DHCPv6 to provide the CGA generation function.

## 2. Coexistence of DHCPv6 and CGA

CGAs can be used with IPv6 Stateless Address Configuration [RFC4862]. The public key system associated with the CGA address provides message origin validation and integrity protection without the need for negotiation and transportation of key materials.

The current CGA specifications do not mandate which device generates a CGA address. In many cases, a CGA address is generated by the associated key pair owner, which normally is also the host that will use the CGA address. However, in a DHCPv6-managed network, hosts should obtain IPv6 addresses only from a DHCPv6 server. This difference of roles needs to be carefully considered if there is a requirement to use CGAs in DHCPv6-managed environments.

The current DHCPv6 specification [RFC3315] has a mechanism that could be used to allow a host to self-generate a CGA for use in a DHCPv6-managed environment, i.e. the DHCPv6 server can grant the use of host-generated CGA addresses on request from the client.

Specifically, a node can request that a DHCPv6 server grants the use of a self-generated CGA by sending a DHCPv6 Request message. This DHCPv6 Request message contains an IA option including the CGA address. Depending on whether the CGA satisfies the CGA-related configuration parameters of the network, the DHCPv6 server can then send an acknowledgement to the node to either grant the use of the CGA or to indicate that the node must generate a new CGA with the correct CGA-related configuration parameters of the network. In the meantime the DHCPv6 server may log the requested address/host combination.

## 3. What DHCPv6 can do for CGA

In the current CGA specifications there is a lack of procedures to enable central management of CGA generation. Administrators should be able to configure parameters used to generate CGAs. DHCPv6 could be used to assign subnet prefixes or certificates to CGA address owners. In some scenarios, the administrator may further want to enforce some parameters, in particular the necessary security-related parameters such as the SEC value.

In the CGA generation procedure, the generation of the Modifier field of a CGA address is computationally intensive. This operation can lead to apparent slow performance and/or battery consumption problems for end hosts with limited computing ability and/or restricted battery power (e.g. mobile devices). In such cases, a mechanism to delegate the computation of the modifier would be desirable. It is possible that the whole CGA generation procedure could be delegated to the DHCPv6 server. This would be especially useful for large SEC values.

Generating a key pair, which will be used to generate a CGA, also requires a notable computation. Generation and distribution of a key pair can also be done by DHCPv6 server. Of course, when designing these new functions, one should carefully consider the impact on security. However, the security considerations of specific solutions are out of scope of this document.

New DHCPv6 options could be defined to carry management parameters from a DHCPv6 server to the client that wishes to use a CGA. A new DHCPv6 prefix assignment option could be defined to propagate a subnet prefix. More DHCPv6 options may be defined to propagate additional CGA-relevant configuration information, such as the SEC value, certificate information, SEND proxy information, etc.

It may be possible to define a delegation operation that allows a client to pass computations to a DHCPv6 server, by introducing new

DHCPv6 option(s). A node could thus initiate a DHCPv6 request to the DHCPv6 server requesting the computation of the Modifier or the CGA. The DHCPv6 server could then either compute the Modifier by itself, or redirect the computation requirement to another server. Once the DHCPv6 server generates (or obtains from the redirected computational server) the Modifier or the CGA address, it can respond to the node with the Modifier or the resulting address and the corresponding CGA Parameters data structure.

Depending on the scenario, the configuration information needed to generate CGAs (including a SEC value, a subnet prefix, a modifier, a public key, a Collision Count value and any Extension Fields) may be provided by either hosts or DHCPv6 servers. A DHCPv6 server might receive from hosts the configuration information customized by hosts, generate CGAs by using configuration information provided by both parties and deliver CGAs and their associated CGA Parameters data structures to hosts. The details of such potential new methods need to be defined clearly in the solution specifications.

New DHCPv6 options may be defined to support the interactions that are required when a DHCPv6 server generates a key pair for hosts.

When designing such solutions, the designer should thoroughly consider the impact on DHCPv6 model and the security of CGA usage. In order to be compatible with DHCPv6, the configuring procedure of CGA parameters should be compatible with the current DHCPv6 definition. When a DHCP6 server configures CGA parameters, integrity protection may be needed to avoid attacks, such as downgrade attack.

## 4. What CGA can do for DHCPv6

DHCPv6 is vulnerable to various attacks, e.g. fake address attacks where a 'rogue' DHCPv6 server responds with incorrect address information. A malicious rogue DHCPv6 server can also provide incorrect configuration to the client in order to divert the client to communicate with malicious services, like DNS or NTP. It may also mount a Denial of Service attack through mis-configuration of the client that causes all network communication from the client to fail. A rogue DHCPv6 server may also collect some critical information from the client. Attackers may be able to gain unauthorized access to some resources, such as network access. See Section 23 [RFC3315].

In the basic DHCPv6 specifications, regular IPv6 addresses are used. However, DHCPv6 servers, relay agents and clients could use CGAs as their own addresses. A DHCPv6 message (from either a server, relay agent or client) with a CGA as source address, can carry the CGA Parameters data structure and a digital signature. The receiver can

verify both the CGA and signature, then process the payload of the DHCPv6 message only if the validation is successful. In this way DHCPv6 messages can be protected. This mechanism can efficiently improve the security of DHCPv6, because the address of a DHCP message sender (which can be a DHCP server, a reply agent or a client) can be verified by a receiver. The usage of CGA can efficiently avoid the above attacks. It improves the communication security of DHCPv6 interactions. The usage of CGA can also avoid DHCPv6's dependence on IPSEC [RFC3315] in relay scenarios. This mechanism is applicable in environments where physical security on the link is not assured (such as over certain wireless infrastructures) or where available security mechanisms are not sufficient, and attacks on DHCPv6 are a concern.

It should be noticed that there could be different levels of pre-configuration of CGA. The minimum level of pre-configuration is to configure public keys on both parties of communication or have a third party authority available for users to retrieve public keys. The public keys will be used for users to generate CGAs and verify CGAs and signatures. The pre-configuration can also include configuring more CGA parameters such as SEC value or more depend on policies. The pre-configuration can even be the whole CGA and related parameters, but in this case the address will be fixed and this situation may not be desired when users want to keep their addresses unknown.

## 5. Security Considerations

As Section 4 of this document has discussed, CGAs can provide additional security features for DHCPv6. However, in defining solutions using DHCPv6 to configure CGAs, as suggested in Section 3. of this document, careful consideration is required to evaluate whether the new mechanism introduces new security vulnerabilities.

When DHCP is used to manage CGAs, CGA relevant information is stored in a central repository, DHCP server. It does not increase privacy risks. The CGA relevant information is only exposed to network management plane. The privacy risks are not higher than other network managed entities, like normal IPv6 addresses managed by DHCP, or addresses log in ACL.

## 6. IANA Considerations

There are no IANA considerations in this document.

## 7. Solution Requests

As discussed in this document, CGAs and DHCPv6 can provide additional services or security features for each other. Solutions that define the details of such interactions should be investigated to determine how viable they are.

## 8. Acknowledgements

Useful comments were made by Marcelo Bagnulo, UC3M, Spain and other members of the IETF CSI working group.

## 9. Change Log [RFC Editor please remove]

draft-jiang-csi-dhacpv6-cga-ps-00, original version, 2008-10-27

draft-jiang-csi-dhacpv6-cga-ps-01, revised after comments at IETF 73, 2009-01-08

draft-jiang-csi-dhacpv6-cga-ps-02, revised after comments at CSI mailing list, 2009-06-17

draft-jiang-csi-dhacpv6-cga-ps-03, revised after comments at CSI mailing list, 2009-09-18

draft-ietf-csi-dhacpv6-cga-ps-00, revised after comments at CSI mailing list and wg adoption call, 2009-10-12

draft-ietf-csi-dhacpv6-cga-ps-01, revised after comments at IETF 76, 2009-12-16

## 10. References

### 10.1. Normative References

[RFC3315] R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins and M. Carney, "Dynamic Host Configure Protocol for IPv6", RFC 3315, July 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", RFC 3972, March 2005.

[RFC4861] T. Narten, E. Nordmark, W. Simpson and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

## 10.2. Informative References

[RFC4339] J. Jeong, Ed., "IPv6 Host Configuration of DNS Server Information Approaches", RFC 4339, February 2006.

Author's Addresses

Sheng Jiang
Huawei Technologies Co., Ltd
KuiKe Building, No.9 Xinxi Rd.,
Shang-Di Information Industry Base, Hai-Dian District, Beijing 100085
P.R. China
Phone: 86-10-82836081
Email: shengjiang@huawei.com

Sean Shen
CNNIC
4, South 4th Street, Zhongguancun
Beijing 100190
P.R. China
Email: shenshuo@cnnic.cn

Tim Chown
University of Southampton
Highfield
Southampton, Hampshire SO17 1BJ
United Kingdom
Email: tjc@ecs.soton.ac.uk