Network Working Group
Internet Draft
Intended status: Standards Track
Expires: August 5, 2010

Sheng Jiang
Huawei Technologies Co., Ltd
Sean Shen
CNNIC

February 5, 2010

Secure DHCPv6 Using CGAs
draft-jiang-dhc-secure-dhcpv6-03.txt

Status of this Memo

Copyright Notice

Abstract

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) enables DHCP servers to pass configuration parameters. It offers configuration flexibility. If not secured, DHCPv6 is vulnerable to various attacks, particularly fake attack. This document analyzes the security issues of DHCPv6 and specifies security mechanisms, mainly using CGAs.

Table of Contents

1. Introduction

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6 [RFC3315]) enables DHCP servers to pass configuration parameters. It offers configuration flexibility. If not secured, DHCPv6 is vulnerable to various attacks, particularly fake attack.

The requirements of using CGA to secure DHCPv6 have been introduced in [PS-DC]. This document analyzes the security issues of DHCPv6 in more details. This document is aiming to provide mechanisms for improving the security of DHCPv6, thus the address of a DHCP message sender, which can be a DHCP server, a reply agent or a client, is able to be verified by a receiver. It improves communication security of DHCPv6 interaction. The security mechanisms specified in this document is mainly based on the Cryptographically Generated Addresses (CGA [RFC3972]).

Secure DHCPv6 is applicable in environments where physical security on the link is not assured (such as over wireless) or where available security mechanisms are not sufficient, and attacks on DHCPv6 are a concern.

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].

3. Security Overview of DHCPv6

DHCPv6 is a client/server protocol that provides managed and stateful configuration of devices. It enables DHCPv6 server to auto-configure relevant network parameters on clients through the DHCPv6 message exchanging mechanisms. In the basic DHCPv6 specifications [RFC3315], security of DHCPv6 message can be improved in a few aspects.

In the basic DHCPv6 specifications, regular IPv6 addresses are used. It is possible for a malicious attacker to use a fake address to spoof or launch an attack.

"One attack specific to a DHCP client is the establishment of a malicious server with the intent of providing incorrect configuration information to the client. The motivation for doing so may be to mount a 'man in the middle' attack that causes the client to communicate with a malicious server instead of a valid server for some service such as DNS or NTP. The malicious server may also mount a denial of service attack through mis-configuration of the client

that causes all network communication from the client to fail." [RFC3315]

"A DHCP client may also be subject to attack through the receipt of a Reconfigure message from a malicious server that causes the client to obtain incorrect configuration information from that server." [RFC3315]

Fake servers can also provide clients with partially correct information that allows the attacker to route traffic through certain host where critical information can be collected. This becomes important to detect and prevent when encrypted traffic is allowed to pass through firewalls. Clients can be configured with bogus data, so that they will assume that the network is down.

Once servers start updating DNS and other directory services, attackers may spoof DHCP servers to register incorrect information in those services.

Another possible attack is that attackers may be able to gain unauthorized access to some resources, such as network access.

The basic DHCPv6 specifications achieve message origin authentication and message integrity via an authentication option with a symmetric key pair. For the key of the hash function, there are two key management mechanisms. Firstly, the key management is out of band, usually manual, i.e. operators set up key database for both server and client before running DHCPv6. Usually multiple keys are deployed once a time and key id is used to specify which key is used. Secondly, a DHCPv6 server sends a reconfigure key to the client in the initial exchange of DHCPv6 messages for future use, in this case security is not guaranteed because this key is transmitted in plaintext. In either way, the security of key itself is in question mark.

Communication between a server and a relay agent, and communication between relay agents, can be secured through the use of IPSec, as described in section 21.1 in [RFC3315]. However, IPSec is quite complicated. A simpler security mechanism may have better deploy ability. Furthermore, the manual configuration and static keys are potential issue makers. Relay agents MAY require other security mechanisms besides IPSec.

4. Secure DHCPv6 Overview

To solve the abovementioned security issues, we introduce CGAs into DHCPv6. CGAs are introduced in [RFC3972]. "CGAs are IPv6 addresses for which the interface identifier is generated by computing a cryptographic one-way hash function from a public key and auxiliary parameters. The binding between the public key and the address can be

verified by re-computing the hash value and by comparing the hash

with the interface identifier. Messages sent from an IPv6 address can be protected by attaching the public key and auxiliary parameters and by signing the message with the corresponding private key. The protection works without a certification authority or any security infrastructure."

In this document, a CGA option with an address ownership proof mechanism and a signature option with a corresponding verification mechanism are introduced. With them, the receiver of a DHCP message can verify the sender address of the DHCP message, which improves communication security of DHCP messages. By using the signature option, the verification of data integrity and replay protections can also be achieved without the authentication option.

This documentation focuses on using CGAs to secure the DHCPv6 protocol. It assumes the sender, which uses CGAs, has self-generated or been configured CGAs. The CGA configuration in the DHCPv6 network is out of scope and specified in [CGA-Conf].

In the relay scenarios, because relay agent restructures the DHCPv6 messages, a receiver would not find the sender's source CGA address in the DHCPv6 message header. In the client-relay-server scenarios, "the relay agent copies the source address from the header of the IP datagram in which the message was received to the peer-address field of the Relay-forward message" [RFC3315]. The receiver, a DHCPv6 server, can find the sender's source CGA address in the peer-address field for CGA verification. In the server-relay-client scenarios, a DHCP server knows a client is behind relay(s) if it receives a Relay-forward DHCPv6 message. Then it will reply a Relay-reply message with the server's source CGA address being carried in the server DUID, which is in the payload. In this way, the receiver, a DHCPv6 client can get the server's source CGA address for CGA verification. The server DUID is also protected by CGA.

4.1. New Components

The components of the solution specified in this document are as follows:

- CGAs are used to make sure that the sender of a DHCPv6 message is the "owner" of the claimed address. A public-private key pair has been generated by a node itself or configured before it can claim an address. A new DHCPv6 option, the CGA Parameter Option, is used to carry the public key and associated parameters.

- Public key signatures protect the integrity of the messages and authenticate the identity of their sender. The authority of a public key is established either with the authorization

delegation process, by using certificates, or through the address ownership proof mechanism, by using CGAs, or with both.

- Server Address type of DUID is used to carry server's source address in the relay scenarios. The receiver gets the server's source CGA address for CGA verification.

4.2. Support for algorithm agility

Hash functions are the fundamental of security mechanisms, including CGAs in this document. "...they have two security properties: to be one way and collision free." "The recent attacks have demonstrated that one of those security properties is not true." [RFC4270]

Following the approach recommended by [RFC4270] and [new-hashes], our analysis shows none of these attacks are currently doable. However, these attacks indicate the possibility of future real-world attacks. Therefore, we have to take into account that future attacks will be improved and provide a support for multiple hash algorithms. Our mechanisms, in this document, support not only hash algorithm agility but also signature algorithm agility.

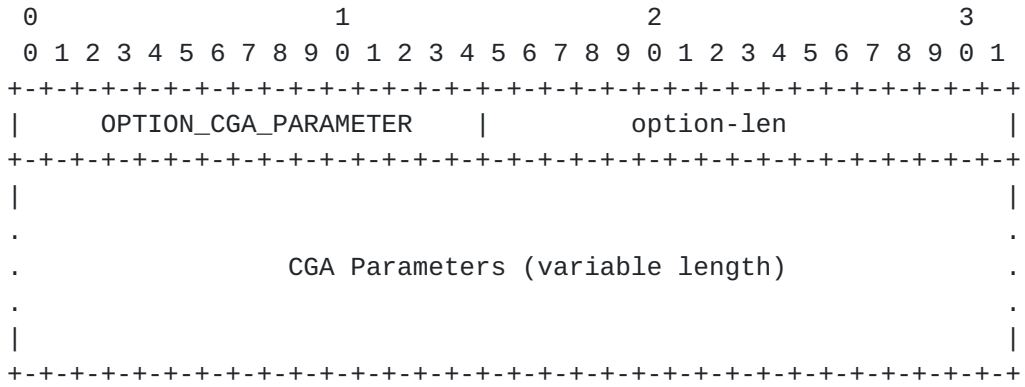
The support for hash agility within CGAs has been defined in [RFC4982]. The usage of CGAs in this document SHOULD also obey [RFC4982], too.

5. Extension for Secure DHCPv6

This section extends DHCPv6. Two new options and a new DUID type have been defined. The new options MUST be supported, if the node has been configured to use Secure DHCPv6. The new DUID type MUST be supported in the relay scenarios.

5.1. CGA Parameter Option

The CGA option allows the verification of the sender's CGAs. The format of the CGA option is described as follows:



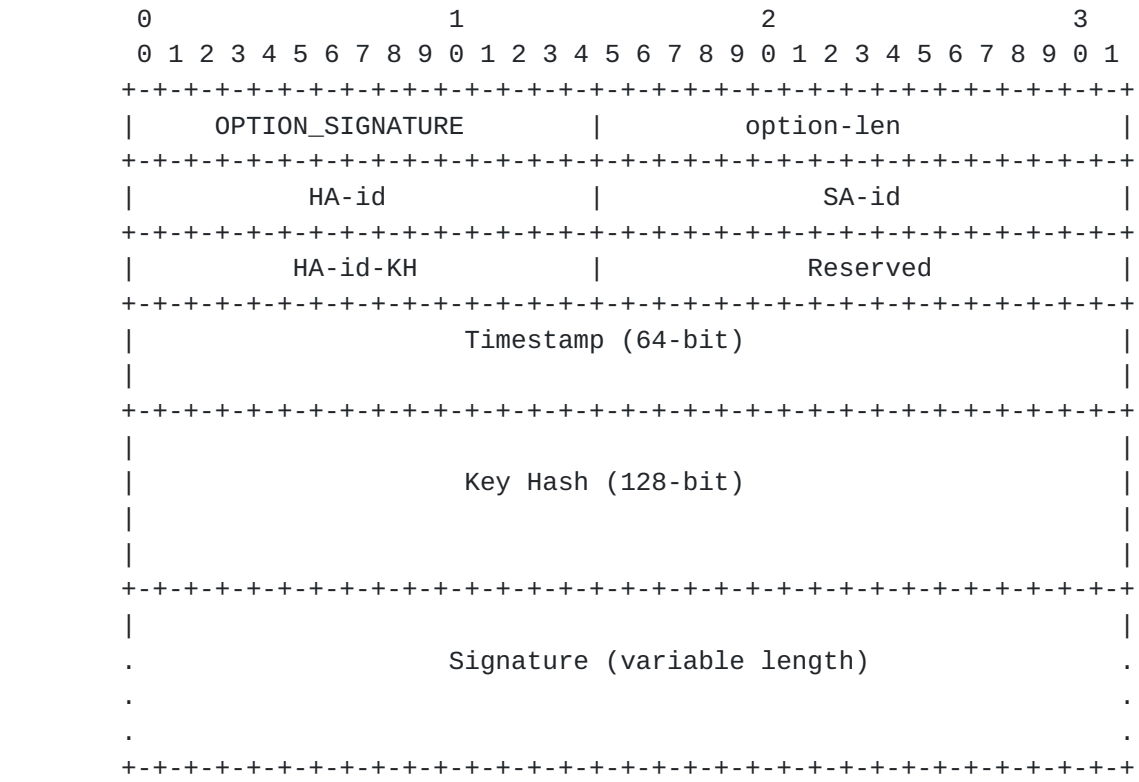
option-code OPTION_CGA_PARAMETER (TBA1).

option-len Length of CGA Parameters in octets.

CGA Parameters A variable-length field containing the CGA Parameters data structure described in Section 4 of [RFC3972]. This specification requires that the public key found from the CGA Parameters field in the CGA option MUST be that referred by the Key Hash field in the Signature option. Packets received with two different keys MUST be silently discarded. Note that a future extension MAY provide a mechanism allowing the owner of an address and the signer to be different parties.

5.2. Signature Option

The Signature option allows public key-based signatures to be attached to a DHCPv6 message. The Signature option COULD be any place within the DHCPv6 message. It protects all the DHCPv6 header and options before it. Any options after the Signature option can be processed, but it should be noticed that they are not protected by this Signature option. The format of the Signature option is described as follows:



option-code OPTION_SIGNATURE (TBA2).

option-len 32 + Length of signature field in octets.

HA-id Hash Algorithm id. The hash algorithm is used for computing the signature result. RSA signature [RSA] with SHA-1 [sha-1] is adopted. In order to provide hash algorithm agility, SHA-1 is assigned an initial value 0x0000 in this document.

SA-id Signature Algorithm id. The signature algorithm is used for computing the signature result. RSA signature with RSASSA-PKCS1-v1_5 algorithm is adopted. In order to provide algorithm agility, RSASSA_PKCS1-v1_5 is assigned an initial value 0x0000 in this document.

HA-id-KH Hash Algorithm id for Key Hash. Hash algorithm used for producing the Key Hash field in the Signature option. SHA-1 is adopted. In order to provide hash algorithm agility, SHA-1 is assigned an initial value 0x0000 in this document.

Reserved A 16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Timestamp The current time of day (NTP-format timestamp [RFC1305], a 64-bit unsigned fixed-point number, in seconds relative to 0h on 1 January 1900.). It can reduce the danger of replay attacks.

Key Hash A 128-bit field containing the most significant (leftmost) 128 bits of a SHA-1 hash of the public key used for constructing the signature. The SHA-1 hash is taken over the presentation used in the Public Key field of the CGA Parameters data structure carried in the CGA option. Its purpose is to associate the signature to a particular key known by the receiver. Such a key can either be stored in the certificate cache of the receiver or be received in the CGA option in the same message.

Signature A variable-length field containing a digital signature. The signature value is computed with the hash algorithm and the signature algorithm, as described in HA-id and SA-id. The signature constructed by using the sender's private key

over the following sequence of octets:

1. The 128-bit CGA Message Type tag value for Secure DHCPv6, 0x81be a1eb 0021 ce7e caa9 4090 0665 d2e0 02c2. (The tag value has been generated randomly by the editor of this specification.).

2. The 128-bit Source IPv6 Address.

3. The 128-bit Destination IPv6 Address.

4. The DHCPv6 message header.

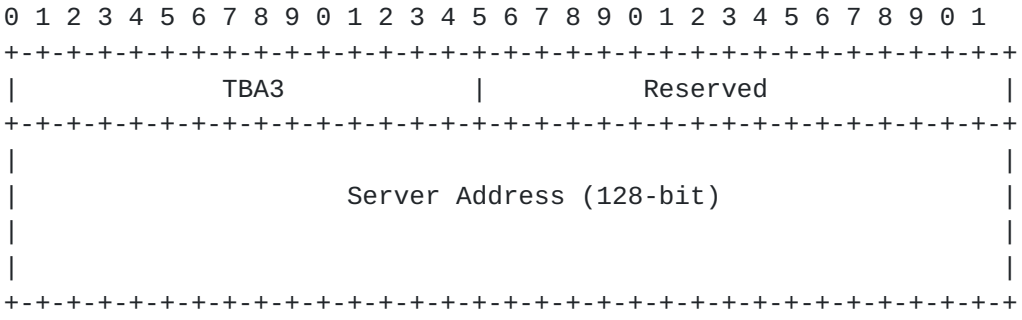
5. All DHCPv6 options except for the Signature option and the Authentication Option.

6. The content between the option-len field and the signature field in this Signature option, in the format described above.

5.3. DUID-SA Type

Server Address Type DUID (DUID-SA) allows IP address of DHCPv6 servers can be carried in DHCPv6 message payload.

The following diagram illustrates the format of a DUID-SA:



Type-code DUID-SA Type (TBA3)

Reserved A 16-bit field reserved for future use. The value MUST be initialized to zero by the sender, and MUST be ignored by the receiver.

Server Address The 128-bit IPv6 address of the DHCPv6 server.

In the secure DHCPv6 solution, the Server Address field of DUID-SA, which is the IPv6 address of the DHCPv6 server, MUST be a CGA.

In the secure DHCPv6 solution, all the payloads, including DUID-SA, are protected by signature option by the definition of section 5.1 and 5.2.

6. Processing Rules and Behaviors

6.1. Processing Rules of Sender

A DHCPv6 node, which could be a server, relay agent or client, can be configured to send Secure DHCPv6 messages only if CGAs have been configured on it.

The node MUST record the following configuration information:

CGA parameters Any information required to construct CGAs, as described in [RFC3972].

Keypair A public-private key pair. The public key used for constructing the signature MUST be the same in CGA parameters.

CGA flag A flag that indicates whether CGA is used or not.

If a node has been configured to use Secure DHCPv6, the node MUST send a message using a CGA, which be constructed as specified in Section 4 of [RFC3972], as the source address unless they are sent with the unspecified source address. In the message, both the CGA option and the Signature option MUST be present in all DHCPv6 messages. The CGA Parameter field in the CGA option is filled according to the rules presented above and in [RFC3972]. The public key in the field is taken from the configuration used to generate the CGA, typically from a data structure associated with the source address. The Signature option MUST be constructed as explained in Section 5.2 and be the last DHCPv6 option.

In relay scenario, a DHCPv6 server MUST include an OPTION_SERVERID [RFC3315] in Relay-reply message and put its CGA in the Server Address field of the DUID in the OPTION_SERVERID. The CGA of DHCPv6 server will not lose during relaying so that the client can verify CGA address and signature.

6.2. Processing Rules of Receiver

The node that supports the verification of the Secure DHCPv6 messages MUST record the following configuration information:

Minbits The minimum acceptable key length for public keys used in the generation of CGAs. The default SHOULD be 1024 bits. Implementations MAY also set an upper limit for the amount of computation

needed when verifying packets that use these security associations. Any implementation SHOULD follow prudent cryptographic practice in determining the appropriate key lengths.

On a node that has been configured to use Secure DHCPv6, DHCPv6 message without either the CGA option or the Signature option MUST be treated as unsecured. Note the Secure DHCPv6 nodes MAY simply discard the unsecured messages.

The receiving node MUST verify the source address of the packet by using the algorithm described in Section 5 of [RFC3972]. The inputs to the algorithm are the source address, as used in IP header, and the CGA Parameters field.

If the CGA verification is successful, the recipient proceeds with a more time-consuming cryptographic check of the signature. Note that even if the CGA verification succeeds, no claims about the validity of the use can be made until the signature has been checked.

The receiving node MUST verify the Signature option as follows: the Key Hash field MUST indicate the use of a known public key, either one learned from a preceding CGA option in the same message, or one known by other means. The signature field verification MUST show that the signature has been calculated as specified in the previous section.

Only the messages that get through both CGA and signature verifications are accepted as secured DHCPv6 messages and continue to be handled for their contained DHCPv6 options.

Messages that do not pass all the above tests MUST be silently discarded if the host has been configured to accept only secured DHCPv6 messages. The messages MAY be accepted if the host has been configured to accept both secured and unsecured messages but MUST be treated as an unsecured message. The receiver MAY also otherwise silently discard packets.

In the relay scenarios, a DHCPv6 server obtains the CGA of a client from the peer address field in the Relay-forward message. A DHCPv6 client obtains the CGA of a server from the Server Address field of the DUID in the OPTION_SERVERID.

6.3. Processing Rules of Relay Agent

To support secure DHCPv6, Relay Agents follow the same processing rules defined in [RFC3315].

By current definition: "The relay agent copies the source address from the IP datagram in which the message was received from the

client into the peer-address field in the Relay-forward message". The CGA of a client will not lose during relaying.

A relay will not change the OPTION_SERVERID when processing Relay-reply message from a DHCPv6 server, CGA of the DHCPv6 server will not lose.

7. Security Considerations

This document provides new security features to the DHCPv6 protocol.

DHCPv6 nodes without CGAs or the DHCPv6 messages that use unspecific addresses cannot be protected.

Downgrade attacks cannot be avoided if nodes are configured to accept both secured and unsecured messages. A future specification MAY provide a mechanism on how to treat unsecured DHCPv6 messages. One simple solution MAY be that Secure DHCPv6 is mandated on all servers, reply agents and clients if a certain link has been deployed Secure DHCPv6.

8. 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 CGA Parameter Option (TBA1), described in Section 5.1.

The Signature Option (TBA2), described in Section 5.2.

This document defines a new DHCPv6 DUID, which MUST be assigned DUID Type values within the DHCPv6 DUID Type numbering space:

The DUID-SA (TBA3), described in Section 5.3.

This document defines three new registries that have been created and are maintained by IANA. Initial values for these registries are given below. Future assignments are to be made through Standards Action [RFC5226]. Assignments for each registry consist of a name, a value and a RFC number where the registry is defined.

Hash Algorithm id(HA-id). The values in this name space are 16-bit unsigned integers. The following initial values are assigned for HA-id in this document:

Name	Value	RFCs
SHA-1	0x0000	this document

Signature Algorithm (SA-id). The values in this name space are 16-bit unsigned integers. The following initial values are assigned for SA-id in this document:

Name	Value	RFCs
SHA-1	0x0000	this document

Hash Algorithm id for Key Hash (HA-id-KH). The values in this name space are 16-bit unsigned integers. The following initial values are assigned for HA-id-KH in this document:

Name	Value	RFCs
RSASSA-PKCS1-v1_5	0x0000	this document

This document defines a new 128-bit value under the CGA Message Type [RFC3972] namespace, 0x81be a1eb 0021 ce7e caa9 4090 0665 d2e0 02c2.

9. Acknowledgments

The authors would like to thank Bernie Volz and other members of the IETF DHC & CSI working groups for their valuable comments.

10. References

10.1. Normative References

[RFC1305] D. Mills, "Network Time Protocol (Version 3) Specification, Implementation and Analysis", RFC1305, March, 1992.

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

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

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

10.2. Informative References

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

[RFC4270] P. Hoffman, B. Schneier, "Attacks on Cryptographic Hashed in Internet Protocols", RFC 4270, November 2005.

[RFC5226] T. Narten, H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, May 2008.

[new-hashes] S.Bellovin, E. Rescorla, "Deploying a New Hash Algorithm", November 2005.

[CGA-Conf] S. Jiang, S. Xia, "Configuring Cryptographically Generated Addresses (CGA) using DHCPv6", draft-jiang-dhc-cga-config-dhcpv6, working in progress, February 2010.

[PS-DC] S. Jiang, et al., "DHCPv6 and CGA Interaction: Problem Statement", draft-ietf-csi-dhcpv6-cga-ps, work in progress, December 2009.

[RSA] RSA Laboratories, "RSA Encryption Standard, Version 2.1", PKCS 1, November 2002.

[sha-1] National Institute of Standards and Technology, "Secure Hash Standard", FIBS PUB 180-1, April 1995, http://www.itl.nist.gov/fipspubs/fip180-1.htm.

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
Email: shengjiang@huawei.com

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