Secure DHCPv6 Using CGAs

draft-jiang-dhc-secure-dhcpv6-02.txt
DHC Working Group
IETF 76, Hiroshima

Sheng JIANG & Sean SHEN

DHCPv6 Security Issues

- **Current DHCPv6 uses regular IPv6 addresses**
  - a malicious attacker can use a fake address to spoof or launch an attack
- **A malicious server can provide incorrect configuration information to the client in order to**
  - cause the client to communicate with a malicious server, like DNS
  - cause all network communication from the client to fail
  - collect critical information through the interaction with clients
- **A malicious client can**
  - spoof DHCP servers to register incorrect information in services, like DNS
  - be able to gain unauthorized access to some resources

Note: we do not analyze all DHCPv6 security issues here, the above are only what we can improve

DHCPv6 Security Issues (2)

- **Current DHCPv6 has defined an authentication option with a symmetric key**
  - its key management using either manual configuration or transmitting key in plaintext
  - 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**
  - IPSec is quite complicated and barely used
  - Communication between a relay agent and a client

Secure DHCPv6 Overview

- **Introduce a CGA option with an address ownership proof mechanism**
  - This CGA address must be used in IP transmission
- **Introduce a signature option with a verification mechanism**
  - The pub/priv key pair with CGA is used for verification/ signature
- **The above two option must be used together**

New DHCPv6 Options

- **CGA Option**
  - containing the CGA Parameters data structure [RFC3972]
- **Signature Option**
  - **HA-id** the hash algorithm is used for computing the signature result
  - **SA-id** the signature algorithm is used for computing the signature result
  - **HA-id-KH** the hash algorithm used for producing the Key Hash field
  - **Timestamp** the current time of day (NTP-format timestamp [RFC1305]), reduce the danger of replay attacks
  - **Key Hash** a 128-bit hash result of the public key used for constructing the signature. To associate the signature to a particular key known by the receiver
  - **Signature** a digital signature constructed by using the sender's private key over CGA Message Type tag, src/des IP addr, DHCPv6 message head and all DHCPv6 options

Processing Rules and Behaviors

- **At the sender side:**
  - send secure DHCPv6 messages using the CGA address
  - both the CGA option and the Signature option MUST be present in all secure DHCPv6 messages
- **At the receiver side:**
  - DHCPv6 messages without either the CGA option or the Signature option MUST be treated as unsecured
  - verify the source address, as used in IP header, with the CGA option
  - verify the Signature option
  - Only the messages that succeed both CGA and signature verifications are accepted as secured DHCPv6 messages

Security Considerations

- **DHCPv6 nodes without CGAs or the DHCPv6 messages that use unspecific addresses as source address cannot be protected**
- **Downgrade attacks cannot be avoided if nodes are configured to accept both secured and unsecured messages**
  - A simple solution is that Secure DHCPv6 is mandated on all servers, reply agents and clients if a certain link has been deployed Secure DHCPv6

Support for Relay Scenarios

- **Relay agent restructures the DHCPv6 messages, new message header does not contain the original sender's source CGA**
  - Client → Relay→ Server

    The relay agent copies the client’s source address to the peer-address field according to [RFC3315]

    The receiver, a DHCPv6 server, can find the sender's source CGA address in the peer-address field for CGA verification.
  - Server → Relay → Client

    The DHCPv6 server will know a client is behind relay(s) by receiving a Relay-forward DHCPv6 message. Then it will reply a Relay-reply message with the server's source CGA being carried in the server DUID
  - The receiver, a DHCPv6 client can get the server's source CGA address for CGA verification. The server DUID is also protected by CGA.
  - The Server Address Type DUID (DUID-SA) is newly defined in this draft. It allows IP address of DHCPv6 servers be carried in DHCPv6 message payload

Discussion on mail list

- **Different from current Auth option?**
- **Can use DHCP Auth framework (use CGA as sub-protocol of current Auth option) ?**
- **Should the Signature option be last or not?**
  - Current draft adopts non-last model
  - Signing all DHCPv6 options except for the Signature option itself and the Authentication Option

Adopt as WG document?

Thank You!

Sheng JIANG (shengjiang@huawei.com)
Sean SHEN (shenshuo@cnnic.com)

Brief Introduce of CGA

- **CGAs [RFC3972] is IPv6 address, which is bound with the public key of the host**
- **The binding between the public key and the address can be verified at the receiver side**
  - Address ownership can be verified
- **Messages sent using CGAs can be protected by attaching the CGA parameters and by signing the message with the corresponding private key of the host**
- **The protection can work via either certificate or local configuration**

Discussion on mail list (1)

- **Different from current Auth option**
  - Source IP address verification
  - Based on simpler but more reliable key management
  - CGA can protects communication between servers and relay agents
  - CGA can be used not particularly for DHCPv6, but also used for other scenarios
- **Why not use DHCP Auth framework (use CGA as sub-protocol of current Auth option)**
  - DHCPv6 AUTH allow only **ONE** auth option, only client and server can authenticate each other, relay agents have to be authenticated via IPSEC
  - Our proposal tries to avoid this IPSEC requirement and makes sure that all the relay agents in the middle can be authenticated and be trusted by the receiver

Discussion on mail list (2)

Should the Signature option be last or not

- **Support to be last (initial design)**
  - Simpler for generator and verifier
  - Last generated in the time order
  - Last in SEND and Enhanced Route Optimization MIPV6
- **Against to be last**
  - None of DHCPv6 option requires specific place
  - Problems if another option also requires to be last in the future
- **It is a design choice, both technically doable**