A Study on Secure Interaction of DHCP Server with DNS Server

YoungHwan Ham*, ByungHo Chung*, KyoIl Chung*
* Information Security Division, Electronics and Telecommunications Research Institute,
161 Gajeong-Dong, Yuseong-Gu, Daejeon, Korea
Tel : +82-42-860-5432 Fax : +82-42-860-5611 E-mail: yhham@etri.re.kr

Abstract: DHCP(Dynamic Host Configuration Protocol) is a protocol which dynamically allocates an IP address and/or host configuration parameters to a host. The DHCP client's address can be changed dynamically any time. For the possible communication with other system, the DHCP client has to inform its address to the DNS system with dynamic update facility. But the DNS dynamic update has a problem related to the security. So we proposed the efficient mechanism for the secure integration of DHCP and DNS by using DNS security extensions. The system also uses the DNS server as the certificate repository for the storing & retrieval of each other's certificate.

1. INTRODUCTION

DHCP is a protocol that dynamically allocates an IP address and/or host configuration parameters to a host. The DHCP is very practical when a administrator manages a lot of network terminal or manages IP addresses of mobile hosts or reuses the only temporarily used IP addresses. The DHCP client, whose address is allocated from DHCP server, has a communication problem with another system, because its address can be changed dynamically any time. For the possible communication with other system, the DHCP client needs the method to inform its address to the other system. The method is to use the DNS system with dynamic update facility, but DNS dynamic update has a problem related to the security. For the secure dynamic update, the DNS system needs a mechanism to authenticate the request of dynamic update from other system [1][2][3]. The DNS with security extensions (RFC2535) can provide integrity and data authentication of the information stored in the DNS server, and integrity and data authentication of DNS queries and responses[5]. By using above DNS extensions and dynamic update, we proposed a secure integration between DHCP and DNS[9][10]. In the public key infrastructure, a user's public key certificate is generated by a certification authority and stored in a directory system. DNS and DHCP server need to authenticate each other by the public key, so they need public key repository system. RFC 2538-"Storing Certificates in the Domain Name System" defines the CERT RR for the storing of public key X.509 certificate[4]. By using this standard, DHCP & DNS server's public key certificate can be stored in the DNS server, and the stored certificate can be retrieved by both server when they need to verify each other's message signature. The DHCP & DNS server can retrieve the necessary certificate in the any other domain because DNS system is already providing naming services world-wide. This paper proposed the interface between DHCP server and DNS repository server, and explains the retrieval mechanism of certificate in the DNS repository.

2. THE SECURE DNS

The secure DNS provides the following three security services.

- Key distribution : Entities such as zones, hosts, and users have a pair of a private key and a public key. The public keys are stored in the DNS server and distributed on demand.
- Integrity and data authentication of the information stored in the DNS server : All the resource records that are the information stored in the DNS server are signed by the DNS server and his signature is stored as a separate resource record.
- Integrity and data authentication of DNS queries and responses : The DNS header and content of a DNS query or response is signed by the private key of the DNS client or DNS server, respectively.

2.1. Key Distribution

All the entities such as zones, hosts, and users have a pair of private key and a public key and the public key is stored as a KEY resource record in the DNS server.

foo.host.examle. IN KEY RDATA

RDATA contains the public key of foo.host.example with the format in Figure 1.

0 15	16 23	24 31
Flags	Protocol	Algorithm
Public Key		

Figure 1. KEY RDATA format

The flag indicates whether the key belongs to a user, a host, or a zone and specifies for what purposes this key can be used. The protocol indicates what protocol including DNS can use this key. The algorithm specifies the asymmetric key algorithm of the public key. The DNS server also stores certificates for entities and CRLs. They are stored as resource records of a CERT type as follow[6].

foo.host.example. CERT RDATA

And RDATA contains following information.

- Type: Specifies whether the certificate is a X.509, SPKI, or PGP type[4].
- Key tag: Specifies which public key in the KEY resource records the public key in this certificate corresponds to.
- Certificate or CRL.

2.2. Integrity and Data Authentication of Resource Records

The integrity and data authentication of resource records in a DNS server are provided basically by SIG resource records. A SIG resource record contains a signature for some other resource record. The signature is made with the private key of the zone which the signed resource record belongs to. A SIG resource record is stored with the following format.

foo.host.example. IN SIG RDATA

And the RDATA contains the following information.

- Type : Specifies whether the type of the signed resource record is an NS, A, MX, or CNAME type.
- Algorithm : Indicates what hash algorithm and symmetric key algorithm are used for the signature.
- Signature expiration : Tells when the signature expires.
- Time signed : Specifies when the signature was made.
- Signer's name
- Signature

When a name server returns a KEY, A, CNAME resource record as an answer, it also sends the corresponding SIG resource record and the resolver receiving the answer checks the integrity of the answer by verifying the signature in the SIG resource record[14][15][16].

2.3. Integrity and Data Authentication of Request/Response

Exchanges of DNS messages which include TSIG [RFC2845] or SIG(0) [RFC2535, RFC2931]records allow two DNS entities to authenticate DNS requests and responses sent between them[7][8]. A TSIG MAC (message authentication code) is derived from a shared secret, and a SIG(0) is generated from a private key whose public counterpart is stored in DNS. In both cases, a record containing the message signature/MAC is included as the final resource record in a DNS message. Keyed hashes, used in TSIG, are inexpensive to calculate and verify. Public key encryption, as used in SIG(0), is more scalable as the public keys are stored in DNS[11][12][13]. A DNS request may be optionally signed by including one SIG(0) at the end of the query additional information section, but DNS update request must be signed by including one SIG(0). It is the request SIG.. Such a SIG is identified by having a "type covered" field of zero. The Transaction SIG(response SIG) is made by signing the preceding DNS request message including DNS header but not including the UDP/IP header. Because the proposed system uses the certificate and need more scalability, the system adapts the SIG(0) method to authenticate the messages.

3. INTEGRATION OF DHCP AND DNS

3.1. The Secure Update of DNS Data

The zone data is signed by zone key and that signature is stored as SIG RR for the purpose of zone data authentication. Besides above zone key, DNS server has its own host key and DHCP server has its own host key which is update key for the pre-configured zone. These key systems are all asymmetric key cryptographic systems and their public key should be shared between DHCP server and DNS server for the support of secure dynamic update of zone data. The DNS server can verify DHCP server host key(zone update key), and DHCP server can verify DNS server's host key. DHCP server sends the update request message with request SIG signed by DHCP host key to DNS server, and then DNS server authenticates request message by DHCP server public key and update the zone data according to the request message. After update of the zone, DNS server signs the zone data by the zone key for the integrity of that updated zone. The DNS server sends response message with transaction SIG (response SIG) signed by its host key to the DHCP server, and then DHCP server authenticates the response message by its DNS server public key.

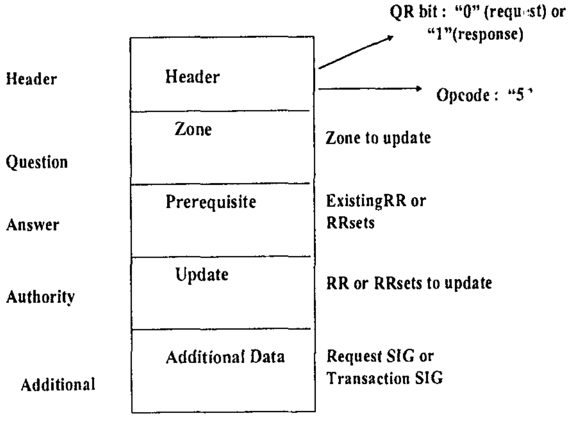

Figure 2. The format of DNS Update Message

The DNS update messages use the extended DNS message format. The Header Section specifies that this message is UPDATE (Opcode:5), and describes the size of the other sections. The Zone Section names the zone that is to be updated by the message. The Prerequisite Section specifies the starting invariants (in terms of zone content) required for this update. The Update Section contains the edits to be made, and the Additional Data Section contains "request SIG" or "transaction SIG" which is created by SIG(0) mechanism explained in the previous section(2.3).

3.2. Interaction Between DHCP and DNS

There are two method of DNS update. The first method is update request of A(address) RR by DHCP client and update request of PTR(pointer query) by DHCP server, because basically DHCP client has domain name to ip mapping and DHCP server has the ip to domain name mapping information. The second method is update request of A RR and PTR RR by DHCP server. In this paper we proposed the second method, because the second method needs only modification of current DHCP server and needs no client modification & overhead. For the client's update request of PTR, the client should have mechanism of authentication and understand the DNS messages. The DNS server should authenticate every DHCP client. Because the advantage of DHCP system is concentrated maintenance of IP address & configuration parameters, it is reasonable that DHCP server is responsible for the update request of A RR and PTR RR.

The DHCP server allocates IP addresses to the clients, and then it requests the update of RR record to the DNS server. For the authentication of DHCP server's update message, DNS server and DHCP server should share the public key for update. Also the two servers should share the public key for authentication of response message.

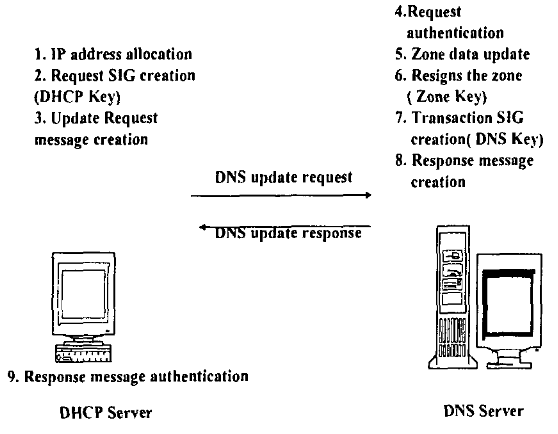
1. IP address allocation
2. Request SIG creation (DHCP Key)
3. Update Request message creation
4.Request authentication
5. Zone data update
6. Resigns the zone (Zone Key)
7. Transaction SIG creation(DNS Key)
8. Response message creation
DNS update request
DNS update response
9. Response message authentication
DHCP Server
DNS Server

Figure 3. The Interaction between DHCP and DNS

The DHCP server should share the public key with only the local DNS server managing its IP address. Even if the DHCP server must interact with non-local DNS server, it can easily retrieve that DNS server's public key by DNS certificate repository system which is explained in the next section. The DNS server need not have a special RR for the authentication of update message, and only should have the DHCP server's host key information.

4. USING DNS AS A CERTIFICATE REPOSITORY FOR INTEGRATED SYSTEM

To retrieve certificates from a DNS server, a DHCP server makes a query message using the resolver library routine (res_mkquery). The operation_code parameter is set to be QUERY. If the DHCP server must interact with the remote DNS server whose certificate is not in the local DNS server, DHCP server can retrieve the remote DNS server's certificate by DNS query and then can verify that certificate by the certificate chain composed by DNS server hierarchy.

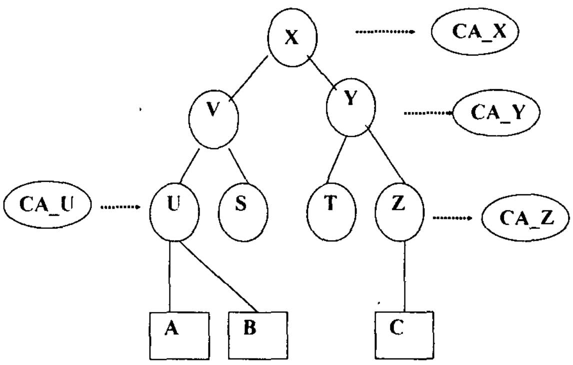

Figure 4. An example hierarchy of DNS servers and certification authorities

Figure 4 shows a hierarchy of DNS servers named S, T, U, V, X, Y, and Z. Among them, the DNS servers, U,X,Y, and Z, have their associated certification authorities. Two users, A and B, are registered in the zone U.V.X and one user C is registered in the zone Z.Y.X. We assume that the user A has the certificates of its own certification authority CA_U and the root certification authority, CA_X. If A wants B's certificate, the query is sent to the DNS server U and U returns B's certificate signed with CA_U's private key. Because A has the public key of CA_U, it can check the validity of the reply.

If A requests the certificate of the user C who is not in the same zone, the request can be processed in an iterative method or a recursive method. In the case of the iterative method, the query is followed as in Figure 5 and each message carries information as follows:

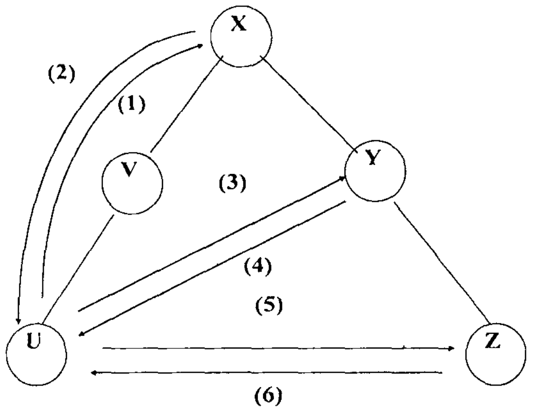

Figure 5. Processing a DNS query in the iterative method

(1) U requests the root DNS server X of C's certificate.
(2) The root returns the address of Y.
(3) U requests Y of C's certificate.
(4) Y returns the address of Z
(5) U requests Z of C's certificate.
(6) Z returns C's certificate

If A wants to check the validity of C's certificate, he needs the certificate path as follows:

CA_X<<CA_Y>>, CA_Y<<CA_Z>>, CA_Z<<CA_C>>

Where
<<X>> = the certificate of the user X issued by certification authority Y

The user A can get this complete certificate path by making each DNS server returns the certificate of its associated certification authority whenever it returns the address of other DNS servers or users' certificates. So X, Y, and Z will return the certificate of CA_X, CA_Y, CA_Z, respectively. Because A has the root certification authority's certificate, the root DNS server need not return the certificate of the root certification authority. All these certificates will be gathered at the user A and the validity of the C's certificate can be verified. C's certificate is stored in the answer section and the certificates of all the certification authorities will be stored in the additional section in the DNS reply message.

In the case of the recursive method, the query is processed as in Figure 6 and each message contains information as follows:

(1) U asks the root server, X, of C's certificate
(2) X asks Y of C's certificate.
(3) Y asks Z of C's certificate.
(4) Z returns C's certificate to Y.
(5) Y relays C's certificate to X.
(6) X relays C's certificate to U.

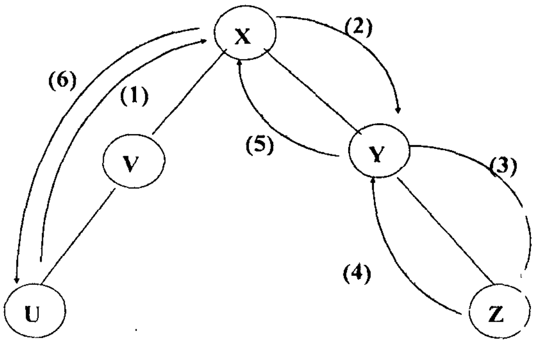

Figure 6. Processing a DNS query in the recursive method

The user A requires the same certificate path as in the iterative method. In can be made possible by making each DNS server append its associated certification authority's certificate when it returns a user certificate or relays an answer. So in our example the user A will find the certificates of CA_X, CA_Y, and CA_Z in the additional section of DNS reply in addition to the certificate of the user C in the answer section of the same DNS reply. In the proposed system, the user A can be local DHCP server and the user C can be remote DNS server managing the local DHCP addresses.

5. CONCLUSION

DHCP server dynamically allocates an IP address and/or host configuration parameters to a DHCP client which have to inform to the other systems if it wants to communicate with other systems with allocated address. The method to inform is to use the DNS system with dynamic update facility, and for the secure dynamic update of DNS system we used DNS with security extensions. When the DNS server allows the dynamic update of RR data, it cannot avoid the weakness of security, but it can interact with other protocols, such as DHCP and provide more flexible service. By using proposed integration mechanism of DHCP and DNS with DNS security extensions and dynamic update, the secure integration can be achieved, and DHCP client system can communicate with other systems freely with its allocated address. The proposed DNS system with secure dynamic update facility can be integrated with other protocols and can provide on line update function to the DHCP server; besides, it can be used as a PKI(Public Key Infrastructure) repository which provides secure directory service and dynamic record update function.

References

[1] Mockapetris P., "Domain Names – Concepts and Facilities", RFC 1034, November 1987.

[2] Mockapetris P., "Domain Names – Implementation and Specification", RFC 1035, November 1987.

[3] R.Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997

[4] R. Housley ., W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile, RFC 2459, January 1999.

[5] D.Eastlake, "Domain Name System Security Extensions", RFC 2535, March 1999

[6] D.Eastlake, "Storing Certificates in the Domain Name System(DNS)", RFC 2538, March 1999.

[7] D.Eastlake, 3rd, "Secret Key Establishment for DNS(TKEY RR)", RFC2930, September 2000.

[8] D.Eastlake, 3rd, "DNS Request and Transaction Signature(SIG(0)s)", RFC 2931, September 2000.

[9] P. Vixie, S. Thomson, Y. Rekhter, "Dynamic Updates in the Domain Name System(DNS UPDATE)", RFC 2136, April 1997.

[10] B.Wellington, "Secure Domain Name System(DNS) Dynamic Update", RFC 3007, November 2000.

[11] D. Eastlake, "RSA/MD5 KEYs and SIGs in the Domain Name System(DNS)", RFC 2537, March 1999.

[12] D. Eastlake, "Storage of Diffie-Hellman Keys in the Domain Name System(DNS)", RFC 2539, March 1999.

[13] P.Vixie, O. Gudmundsson, D. Eastlake 3rd, "Secret Key Transaction Authentication for DNS(TSIG), RFC2845, May 2000.

[14] E.Lewis, "DNS Security Extension Clarification on Zone Status", RFC 3090, March 2001.

[15] D. Eastlake, "DNS Operational Security Considerations", RFC 2541, March 1999.

[16] E.Lewis, "Notes from the State-Of-The-Tech nology:DNSSEC", RFC 3130, June 2001.