JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 4 : 747~754 Apr. 2016

네트워크 공격 방지를 지원하는 DHCP의 설계 및 구현에 관한 연구

유권정 · 김은기*

Design and Implementation of DHCP Supporting Network Attack Prevention

Kwon-joeong Yoo · Eun-gi Kim*

Department of Information and Communication Engineering, Hanbat National University, Daejeon 34158, Korea

요 약

DHCP(Dynamic Host Configuration Protocol)는 IP 주소 관리의 효율성과 편의를 위한 프로토콜이다. DHCP는 네트워크 내 개별 호스트에게 TCP/IP 통신을 실행하기 위해 필요한 IP 주소 및 구성 정보를 자동적으로 할당해준다. 하지만 기존의 DHCP는 서버와 클라이언트 간 상호 인증 체계가 없기 때문에 DHCP spoofing, release 공격과 같은 네트워크 공격에 취약하다. 이러한 문제점을 해결하기 위해 본 논문에서는 다음과 같은 기능을 지원하는 DHCP 프로토콜을 설계하였다. 먼저, ECDH(Elliptic Curve Diffie-Hellman)를 이용하여 세션 키를 생성하고 ECDSA(Elliptic Curve Digital Signature Algorithm)를 사용하여 전자서명을 함으로써 서버와 클라이언트 간 상호 인증을 수행한다. 그리고 메시지에 HMAC(Hash-based Message Authentication Code)을 추가하여 메시지의 무결성을 보장한다. 또한 Nonce를 사용하여 재전송공격을 방지한다. 결과적으로 수신자는 인증되지 않은 호스트로부터 수신한 메시지를 폐기함으로써 네트워크 공격을 막을 수 있다.

ABSTRACT

DHCP(Dynamic Host Configuration Protocol) is a protocol for efficiency and convenience of the IP address management. DHCP automatically assigns an IP address and configuration information needed to run the TCP/IP communication to individual host in the network. However, existing DHCP is vulnerable for network attack such as DHCP spoofing, release attack because there is no mutual authentication systems between server and client. To solve this problem, we have designed a new DHCP protocol supporting the following features: First, ECDH(Elliptic Curve Diffie-Hellman) is used to create session key and ECDSA(Elliptic Curve Digital Signature Algorithm) is used for mutual authentication between server and client. Also this protocol ensures integrity of message by adding a HMAC(Hash-based Message Authentication Code) on the message. And replay attacks can be prevented by using a Nonce. As a result, The receiver can prevent the network attack by discarding the received message from unauthorized host.

키워드 : DHCP, ECDH, ECDSA, HMAC, 네트워크 공격

Key word : DHCP, ECDH, ECDSA, HMAC, network attacks

Received 21 January 2016, **Revised** 17 February 2016, **Accepted** 09 March 2016

* **Corresponding Author** Eun-Gi Kim(E-mail:egkim@hanbat.ac.kr, Tel:+82-42-821-1215)
Department of Information and Communication Engineering, Hanbat National University, Daejeon 34158, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.4.747 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

DHCP(Dynamic Host Configuration Protocol)는 표준 TCP/IP 호스트 설정 프로토콜로, 하나의 클라이언트만을 포함하는 홈 네트워크부터 회사 수준의 인터 네트워크에 이르기까지 모든 부문에서 사용된다[1-4].

기존의 DHCP는 클라이언트와 서버 간 상호 인증을 하지 않으므로 DHCP 해제 공격(release attack), 악성 DHCP 공격(rogue DHCP attack), 재전송 공격(replay attack), DHCP 스푸핑 공격(spoofing attack) 등 네트워크 공격에 노출되어 있다[5]. 본 논문에서는 DHCP를 안전하게 이용하기 위해서 기존의 DHCP 메시지에 인증 기능을 지원하는 옵션을 추가하였다.

본 논문에서는 ECDH(Elliptic Curve Diffie-Hellman)를 이용하여 세션 키를 생성하고 ECDSA(Elliptic Curve Digital Signature Algorithm)를 이용하여 전자서명을 수행함으로써 상호 인증을 한다. 그리고 HMAC(Hash-based Message Authentication Code)을 이용하여 데이터의 무결성을 보장한다[6-8].

기존의 DHCP 인증 방식 중 사용자 ID 기반 인증 보안 방식은 HMAC-MD5 알고리즘을 사용하지만[9] 본 논문에서는 제안하는 DHCP는 ECDH를 사용함으로써 더욱 안전한 상호 인증 기능을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 ECDH 키 교환 알고리즘, ECDSA, HMAC에 대하여 설명하고 3장에서는 DHCP 메시지 옵션의 설계에 대하여 기술한다. 4장에서는 기존의 DHCP와 본 논문에서 제안하는 DHCP에 각각 DHCP spoofing 공격을 통한 성능 검증을 보여준다. 마지막으로 5장에서는 결론을 다룬다.

Ⅱ. 본 연구를 위한 보안 알고리즘

2.1. ECDH 키 교환 알고리즘

ECDH는 DH(Diffie-Hellman) 키 교환 알고리즘에 타원 곡선 암호 방식인 ECC(Elliptic Curve Cryptography) 을 적용한 키 교환 알고리즘이다. ECC 방식을 사용함으로써 기존의 DH 알고리즘과 같은 키 길이에 비해 더 강한 안전성을 보장한다[10].

사용자 A와 B는 각각의 개인키 K_A와 K_B를 생성한다. 타원 곡선 상의 기점을 G라고 가정하였을 때, 사용자 A는 자신의 개인키 K_A와 G를 이용하여 공개키 a를 계산하고, 사용자 B는 자신의 개인키 K_B와 G를 이용하여 공개키 b를 계산한다. 사용자 A와 B는 자신의 공개키 a와 b를 서로에게 전송한다. 사용자 A는 사용자 B로부터 공개키 b를 수신하고 자신의 개인키 K_A와 계산하여 세션 키 S를 얻는다. 마찬가지로 사용자 B는 사용자 A로부터 공개키 a를 수신하여 자신의 개인키 K_B와 계산하여 사용자 A와 사용자 B만 아는 공통의 세션 키 S를 얻는다. 그림 1은 ECDH 키 교환 알고리즘을 이용하여 세션 키를 생성하는 과정을 나타낸다[11,12].

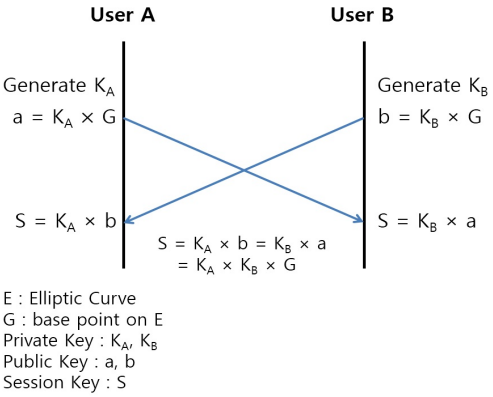

Fig. 1 Session key generation process using ECDH

2.2. ECDSA

ECDSA는 DSA(Digital Signature Algorithm)에 ECC 방식을 적용한 알고리즘이다[11-15]. 그림 2는 송신자가 ECDSA를 이용하여 전자 서명을 생성하고, 수신자가 전자 서명을 검증하는 과정을 나타낸다.

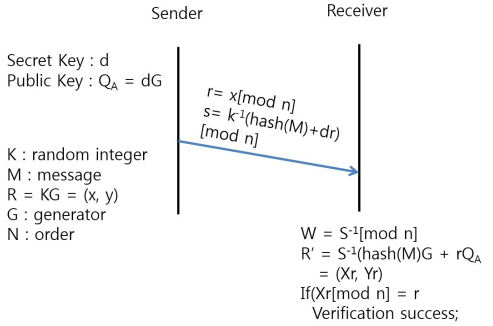

Fig. 2 Digital signature generation and verification using ECDSA

2.3. HMAC

HMAC은 사용자의 비밀 키와 메시지를 해시 함수에 입력하여 해시 코드로, 메시지의 무결성을 보장하는데 사용된다[12,16,17]. 본 논문에서는 ECDH를 이용하여 생성한 세션 키를 해시함수의 비밀 키로 사용한다.

송신자는 HMAC 파라메타로 메시지와 세션 키를 사용하여 HMAC을 생성한다. 송신자는 메시지 뒤에 HMAC을 추가하여 수신자에게 전송한다. 그림 3은 HMAC 함수를 이용하여 HMAC을 생성하는 과정을 나타낸다.

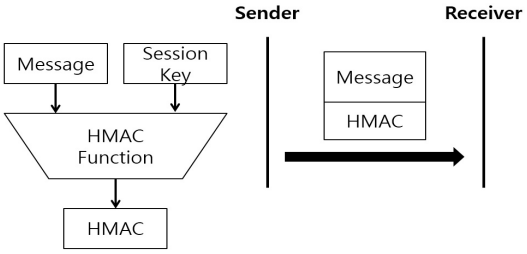

Fig. 3 HMAC generation process

수신자는 수신한 메시지와 자신의 세션 키를 이용하여 HMAC을 생성하고 메시지에 있는 HMAC과 비교하여 메시지의 무결성을 검증한다. 그림 4는 HMAC 함수를 이용하여 HMAC을 검증하는 과정을 나타낸다.

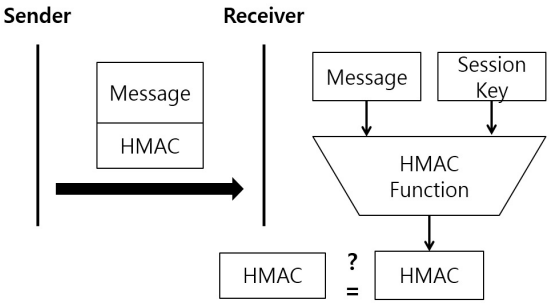

Fig. 4 HMAC verification process

Ⅲ. 제안하는 DHCP의 동작 및 메시지

3.1. 메시지 옵션의 형식

그림 5는 DHCP 메시지 옵션의 형식을 나타낸다. 옵션에 사용되는 값은 4장에서 자세히 서술한다.

Code	Length	Algorithm	Authentication Information

Fig. 5 DHCP message options format

길이 필드(Length)는 알고리즘(Algorithm)과 인증 정보(Authentication Information) 필드의 데이터 길이를 옥텟(Octets)으로 표기한다.

3.2. 동작 과정

클라이언트는 서버로부터 IP 주소를 임대 받기 위해 알고리즘을 협상하고 ECDH를 이용한 키 교환 과정을 거친다. 여기서 임대란 서버가 클라이언트에게 임의의 시간동안 사용할 수 있는 IP 주소를 할당해 주는 것을 말한다[2]. 다음 그림 6은 본 연구에서 제안하는 DHCP의 동작 과정에 따라 사용되는 메시지의 흐름을 나타낸 그림이다.

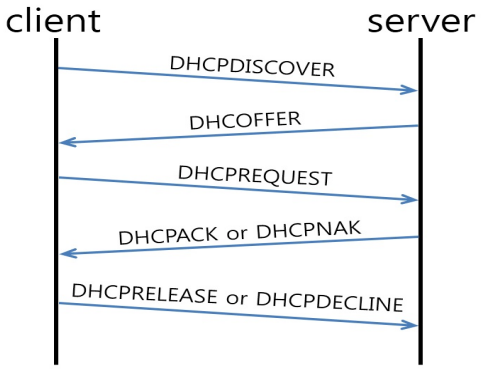

Fig. 6 Process of IP address lease and release

3.2.1. 알고리즘 협상

DHCPDISCOVER 메시지는 클라이언트가 연결할 서버를 찾기 위해 사용되는 메시지이다. 클라이언트가 사용 할 수 있는 ECDH 키 길이와 HMAC 종류를 DHCPDISCOVER 메시지의 옵션으로 설정하여 브로드 캐스트로 전송한다.

DHCPDISCOVER 메시지를 수신한 서버는 해당 메시지의 알고리즘 필드에 있는 알고리즘 중에서 사용할 알고리즘을 선택하고, DHCPOFFER 메시지의 인증 정보 필드에 Nonce와 전자 서명을 포함시켜 클라이언트에게 전송한다[2, 6]. Nonce가 없는 경우에는 서버의 전자서명이 포함된 메시지로 재전송 공격이 이루어 질 수

있기 때문에 서버가 전자서명을 생성할 때 Nonce를 포함하여 재전송 공격을 방지한다. 다음 그림 7은 알고리즘 협상 시에 사용되는 메시지 옵션이다.

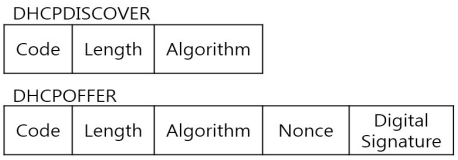

Fig. 7 Message option in algorithm negotiation process

3.2.2. IP 주소 임대 과정

DHCPOFFER 메시지를 수신한 클라이언트는 DHCPREQUEST 메시지를 서버에게 전송한다[2,7]. 이때 메시지의 인증 정보 필드는 서버가 선택한 알고리즘을 이용하여 생성한 ECDH 공개키로 구성된다. 서버가 DHCPREQUEST 메시지를 수신하면 DHCPACK 또는 DHCPNAK 메시지로 응답한다[2,7].

서버가 DHCPACK 메시지를 전송하는 경우에는 메시지의 인증 정보 필드에 서버의 공개키, Nonce, 전자서명을 포함시킨다. 클라이언트가 DHCPACK 메시지를 수신하면 클라이언트와 서버가 서로의 공개키를 알게 됨으로써 서버와 클라이언트는 수신한 상대방의 공개키와 자신의 개인키를 ECDH 키 알고리즘으로 계산하여 서로만 아는 세션 키를 생성할 수 있다. 이를 이용하여 클라이언트는 상대가 올바른 서버임을 검증 한 후 서버로부터 임대 받은 주소를 검사한다. 임대 받은 주소가 사용 중이지 않으면 나머지 IP 주소 임대 과정을 완료한다. 임대 받은 주소가 이미 사용 중인 경우는 3.2.3절에서 설명한다. 서버가 DHCPNAK 메시지를 전송하는 경우에는 메시지의 인증 정보 필드에 Nonce와 전자 서명을 포함시킨다. 그림 8은 IP 주소 임대 과정에서 사용되는 메시지 옵션을 나타낸다.

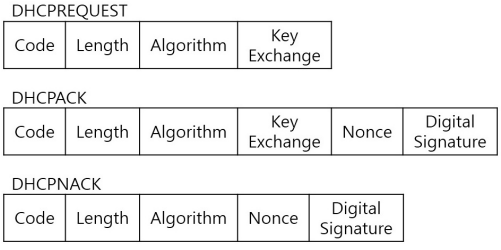

Fig. 8 Message option in IP address lease process

3.2.3. IP 주소 임대 해제 과정

클라이언트가 정상적으로 IP 주소의 사용을 마치는 경우에는 세션 키를 이용하여 만든 HMAC을 메시지의 인증 정보 필드에 포함하여 DHCPRELEASE 메시지를 서버에게 전송한다. 또는 임대 받은 주소가 이미 사용 중이면 생성한 HMAC을 메시지의 인증 정보 필드에 포함하여 서버에게 DHCPDECLINE 메시지를 전송한다. 클라이언트는 DHCPDECLINE 또는 DHCPRELEASE 메시지를 전송한 뒤 세션 키를 삭제하고 IP 주소 임대 과정을 완료한다. 그림 9는 IP 주소 임대 해제 시 사용되는 메시지 옵션이다.

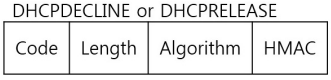

Fig. 9 Message option in IP address release process

서버가 DHCPDECLINE 메시지를 수신한 경우에 해당 IP 주소를 관리자에게 알린다. DHCPRELEASE 메시지를 수신한 경우에는 해당 IP 주소에 대한 임대를 정상적으로 해제한다. 각 과정 이후에는 기존의 세션 키를 삭제한 후 새로운 클라이언트의 DHCPDISCOVER를 기다린다.

3.2.4. 재 임대 과정

클라이언트가 재부팅하거나 네트워크를 재시작할 때 이전의 임대받은 정보를 가지고 있다면 재 임대 과정을 수행한다[18]. 재 임대 과정은 임대 과정에서 3.2.1절에 해당하는 알고리즘 협상 과정을 제외한 나머지 동작과 같다. 재 임대 과정에서 사용하는 메시지 옵션은 3.2.2절에서 설명한 IP 주소 임대 과정의 메시지 옵션과 같다.

3.2.5. 임대 갱신 과정

클라이언트는 IP 주소 임대 과정 또는 재 임대 과정이 완료될 때 두 개의 타이머를 설정한다. 일반적으로 갱신 타이머는 임대 기간의 50%, 리바인딩 타이머는 임대 기간의 87.5%로 설정한다[18]. 여기서 리바인딩이란 임대 갱신에 실패하고 새로운 서버를 찾는 것을 의미한다. 클라이언트는 갱신 타이머가 만료되면 임대를 연장하고, 새로운 세션 키를 갱신하기 위해서 DHCPREQUEST 갱신 메시지를 서버에게 전송한다.

이때 DHCPREQUEST 갱신 메시지는 클라이언트의 새로운 공개키와 이전의 세션 키로 생성한 HMAC을 포함한다. 그림 10은 갱신 과정에서 DHCPREQUEST 메시지에 사용되는 옵션을 나타낸다.

Fig. 10 DHCPREQUEST message option in lease renewal process

서버가 DHCPREQUEST 갱신 메시지를 수신하면 이전의 세션 키로 HMAC을 생성하여 올바른 클라이언트임을 인증하고 DHCPACK 또는 DHCPNAK 메시지를 클라이언트에게 전송한다. 갱신 과정에서 DHCPACK 메시지와 DHCPNAK 메시지의 옵션은 3.2.2절에서 설명한 IP 주소 임대 과정에서 사용하는 옵션과 동일하다.

서버가 DHCPACK 메시지를 전송하는 경우에는 자신의 새로운 ECDH 공개키, Nonce, 전자 서명을 포함하여 전송한다. 그리고 이전의 세션 키를 삭제하고 새로운 세션 키를 저장한다. 클라이언트가 서버로부터 DHCPACK 메시지를 수신하면 갱신 타이머와 리바인딩 타이머를 재설정한다. 이때 이전의 세션 키를 삭제하고 새로운 세션 키를 저장한 뒤 나머지 IP 주소 임대 과정을 완료한다.

서버가 DHCPNAK 메시지를 전송하는 경우에는 Nonce, 전자 서명을 포함하여 전송하고 이전의 세션 키를 삭제한 뒤, 새로운 클라이언트의 DHCPDISCOVER를 기다린다. 클라이언트가 DHCPNAK 메시지를 수신하면 이전의 세션 키를 삭제하고 IP 주소 임대 과정을 종료한다. 임대 갱신 과정에서 송수신 하는 메시지는 그림 11과 같다.

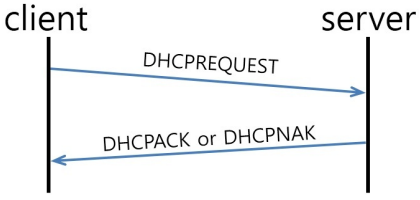

Fig. 11 Message in lease renewal process

3.2.6. 리바인딩 과정

갱신 과정에서 임대를 연장하지 못하면 리바인딩 타이머가 만료되며, 클라이언트는 새로운 서버를 찾고 세션 키를 갱신하기 위해서 DHCPREQUEST 리바인딩 메시지를 서버들에게 전송한다. DHCPREQUEST 리바인딩 메시지는 클라이언트의 새로운 공개키를 포함한다. 새로운 서버가 DHCPREQUEST 갱신 메시지를 수신하면 DHCPACK 또는 DHCPNAK 메시지를 클라이언트에게 전송한다. 서버가 DHCPACK 메시지를 전송하는 경우에는 자신의 새로운 ECDH 공개키, Nonce, 전자 서명을 포함하여 전송하고 세션 키를 저장한 뒤 나머지 과정을 수행한다. 또는 DHCPNAK 메시지를 전송하는 경우에는 Nonce, 전자 서명을 포함시켜 전송하고 새로운 클라이언트의 DHCPDISCOVER를 기다린다. 리바인딩 과정에서 사용하는 메시지 옵션은 3.2.2절의 그림 8과 같다.

Ⅳ. 제안하는 DHCP 메시지 옵션의 구조

본 논문에서는 2장에서 제시된 보안 알고리즘들을 지원할 수 있도록 하며, 이를 위하여 그림 5와 같은 DHCP 메시지 옵션 구조를 추가하였다.

4.1. 메시지 옵션의 구조 및 설정 값

옵션 코드(Code)는 기존의 DHCP에 정의되어 있지 않은 번호인 222를 사용한다[3]. 알고리즘 필드는 2 Bytes의 길이로 상위 1 Byte에는 ECDH 키 길이에 따라 값을 설정하고, 하위 1 Byte에는 HMAC의 종류에 따라 값을 설정한다. 표 1은 알고리즘 필드의 상위 1 Byte에 사용되는 ECDH의 키 길이와 그에 대응하는 값을 나타낸다.

Table. 1 Setting value according to the ECDH key length

Key exchange method	Value(binary)	Key length(bits)
EMPTY	0000 0000	-
ECDH	0000 0001	256
	0000 0010	384
	0000 0100	521
EMPTY	0000 1000	-
	0001 0000	-
	0010 0000	-
	0100 0000	-
	1000 0000	-

표 2는 알고리즘 필드의 하위 1 Byte가 나타내는 값으로, HMAC 종류와 그에 대응하는 값을 나타낸다.

Table. 2 Setting value according to the HMAC type

HMAC type	Value(binary)	Output length(bit)
EMPTY	0000 0000	-
SHA256	0000 0001	256
SHA384	0000 0010	384
SHA512	0000 0100	512
EMPTY	0000 1000	-
	0001 0000	-
	0010 0000	-
	0100 0000	-
	1000 0000	-

인증 정보 필드는 ECDH 공개키, HMAC, Nonce [19], ECDSA로 이루어진다. 또한 인증 정보 필드는 메시지의 종류에 따라 선택적으로 사용된다. Nonce는 2 Bytes이며 상위 1 Byte는 랜덤 값, 하위 1 Byte는 순서 번호(Sequence number)로 구성된다.

Ⅴ. 동작 검증

동작 검증을 설명하기 전에 DHCP 스푸핑 공격이란 공격자가 게이트웨이(default gateway) 주소를 위조하여 클라이언트에게 메시지를 전송함으로써 클라이언트의 메시지를 도청하게 되는 공격을 말한다.

다음은 와이어샤크(wireshark) 프로그램을 이용하여 기존의 DHCP와 본 논문에서 제안하는 DHCP에 각각 DHCP 스푸핑 공격을 한 모습과 그 과정을 설명하고 차이점을 설명한다.

본 논문에서 정상적인 서버의 IP 주소는 192.168.0.2이고, 공격자의 IP 주소는 192.168.0.7이다. 또한 서버가 제공하는 기본 게이트웨이 주소는 192.168.0.1로 가정한다. 기존의 DHCP에 DHCP 스푸핑 공격을 했을 때 전송되는 패킷들은 다음 그림 12와 같다.

Source	Destination	Protocol	Length	Info
0.0.0.0	255.255.255.255	DHCP	349	DHCP Request
192.168.0.2	255.255.255.255	DHCP	582	DHCP ACK
192.168.0.2	192.168.0.9	DHCP	457	DHCP ACK

Fig. 12 DHCP spoofing attack on the existing DHCP

클라이언트는 IP 주소가 192.168.0.2인 서버와 통신한다는 내용을 포함한 DHCPREQUEST 메시지를 브로드캐스트로 전송한다. 다음 그림 13은 DHCPREQUEST 메시지에 포함된 클라이언트가 통신하기를 원하는 서버의 IP 주소이다.

```
▽ Option: (54) DHCP Server Identifier
    Length: 4
    DHCP Server Identifier: 192.168.0.2 (192.168.0.2)
```

Fig. 13 IP address of server selected by client

공격자는 수신한 DHCPREQUEST 메시지를 통해 클라이언트와 통신 할 서버를 확인하고 거짓 DHCPACK 메시지를 생성한다. 이 때 DHCPACK의 옵션 중 기본 게이트웨이 주소를 자신의 IP 주소로 설정하여 클라이언트에게 전송한다. 그리고 클라이언트와 통신할 서버도 클라이언트에게 정상적인 DHCPACK 메시지를 전송한다. 다음 그림 14와 그림 15는 각 정상적인 서버와 공격자의 DHCPACK에 포함된 게이트웨이 주소이다.

```
▽ Option: (3) Router
    Length: 4
    Router: 192.168.0.7 (192.168.0.7)
```

Fig. 14 Default gateway address provided by attacker

```
▽ Option: (3) Router
    Length: 4
    Router: 192.168.0.1 (192.168.0.1)
```

Fig. 15 Default gateway address provided by server

공격자의 DHCPACK 메시지가 클라이언트에게 먼저 도착했을 경우에 클라이언트는 DHCPACK 메시지의 IP 주소가 자신과 통신 할 서버의 IP 주소와 동일하기 때문에 공격자라는 것을 알지 못한다. 따라서 클라이언트는 자신의 기본 게이트웨이 주소를 공격자의 거짓 DHCPACK 메시지에 있는 게이트웨이 주소로 설정한다. 결과는 그림 16과 같이 콘솔에서 route 명령어를 통해 확인 할 수 있다.

```
[root@localhost ~]# route
Kernel IP routing table
Destination     Gateway         Genmask
default         192.168.0.7     0.0.0.0
192.168.0.0     0.0.0.0         255.255.255.0
```

Fig. 16 Routing tables after successful DHCP spoofing attack

본 논문이 제안하는 DHCP에 DHCP 스푸핑 공격을 했을 때 클라이언트는 수신한 DHCPACK 메시지에 있는 전자서명에 포함 된 서버의 공개키를 이용하여 올바른 서버인지 검증 할 수 있다. 올바른 서버일 경우에 클라이언트는 자신의 기본 게이트웨이 주소를 서버가 제공하는 게이트웨이 주소로 설정한다. 그렇지 않을 경우에는 해당 DHCPACK 메시지를 폐기한다.

다음 그림 17은 클라이언트가 수신한 DHCPACK 메시지를 검증 후 올바른 서버가 제공하는 게이트웨이 주소로 자신의 기본 게이트웨이 주소를 설정한 모습이다.

```
[root@localhost ~]# route
Kernel IP routing table
Destination     Gateway         Genmask
default         192.168.0.1     0.0.0.0
192.168.0.0     0.0.0.0         255.255.255.0
```

Fig. 17 Routing tables after DHCP spoofing attack

Ⅵ. 결 론

본 논문에서는 네트워크 공격을 방지하기 위해 DHCP 임대 과정에서 서버와 클라이언트의 상호 인증을 수행하고, 메시지의 무결성을 보장하는 DHCP 메시지 옵션을 제안하였다.

서버는 ECDSA를 이용하여 생성한 전자 서명을 서버가 전송하는 모든 메시지에 포함하여 자신이 올바른 서버임을 인증한다. 또한 서버와 클라이언트는 ECDH 키 교환 알고리즘을 이용하여 공통의 세션 키를 생성한다. 키 교환이 완료된 이후 클라이언트는 세션 키로 생성한 HMAC을 메시지에 포함하여 전송함으로써 클라이언트의 인증과 메시지의 무결성을 보장한다.

기존의 DHCP 스푸핑 공격에 대한 방어 대책은 이미 연결한 서버 이외의 모든 포트(port)를 닫음으로써 통신을 차단하는 것이다. 이 방안은 공격자의 DHCPACK 메시지가 서버의 DCHPACK 메시지보다 클라이언트에게 먼저 도착했을 경우에 공격을 막을 수 없다. 하지만 본 연구에서 제안한 DHCP는 클라이언트가 서버로부터 IP 주소를 임대 받을 때 두 호스트 간 상호 인증을 수행하므로 수신되는 메시지의 순서에 상관없이 인증되지 않은 호스트의 메시지는 폐기하여 DHCP 스푸핑 공격을 막아낼 수 있다. 또한 메시지 옵션에 Nonce를 추가하여 재전송 공격을 막아낼 수 있을 뿐만 아니라 두 호스트간의 상호 인증을 수행함으로써 DHCP 해제 공격(release attack), 악성 DHCP 공격(rogue DHCP attack) 등을 막아낼 수 있을 것으로 예상된다.

추후에는 본 논문의 결과를 이용하여 DHCP 및 관련 프로토콜의 공격 방지에 관한 추가적인 연구를 수행할 예정이다.

REFERENCES

[1] Charles M. Kozierok, *TCP / IP Complete Guide*, Uiwang:acorn publishing Co., 2007.

[2] IETF Std. RFC 2131, *Dynamic Host Configuration Protocol*, IETF, R. Droms, March 1997.

[3] Behrouz A. Forouzan, *TCP/IP Protocol Suite*, Fourth Edition. New York, NY: McGRAW HILL INTERNATIONAL EDITION, 2010.

[4] Won-jong Kang, Jung-jae Yoon, and Chan Koh, “Effective IP Address Management on Ethernet Environment,” *The Korean Society for Industrial and Applied Mathematics*, vol. 7, no. 2, pp113-125, Dec. 2003

[5] IETF. Privacy considerations for DHCP, draft-ietf-dhc-dhcp-privacy-00 [Internet]. Available: https://datatracker.ietf.org/doc/draft-ietf-dhc-dhcp-privacy/00/.

[6] IETF Std. RFC 2132, *DHCP Options and BOOTP Vendor Extensions*, IETF, S. Alexander, R. Droms, March 1997.

[7] IETF Std. RFC 3118, *Authentication for DHCP messages*, IETF, R. Droms, W. Arbaugh, June 2001.

[8] Moon-Gi Kim, Da-Hye Jeong Jae-Won Lee, Kwon-Jeong Yoo, Eun-Gi Kim, “A Study on the DHCP Supporting Network Attack Prevention,” in *The 2015 Fall Conference of the KIPs*, Jeju, pp. 1-3, 2015.

[9] IETF Std. RFC 3118, *Authentication for DHCP Messages*, IETF, R. Droms, Editor, W. Arbaugh, Editor, June 2001.

[10] Carlisle Adams and Steve Lloyd, *Effective way for security PKI*, Seoul, Infobook, 2003.

[11] Seok-ho Kim, “Comparison and analysis on efficiency of scalar multiplication for Elliptic Curve Cryptosystem,” M. S. dissertation, Korea Maritime and Ocean University graduate school, Busan, 2003.

[12] Yeong-ja Kim, “Design and implementation of a security messenger system using elliptic curve cryptosystem,” M. S. dissertation, Chung-Ang University Information graduate school, Seoul, 2004.

[13] IETF Std. RFC 6979, *Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA)*, IETF, T. Pornin, August 2013.
[14] Song-hwan Lim, “The efficiency analysis of ECDSA using improved element algorithm,” M. S. dissertation, Dongguk University Graduate School of International Affairs & Information, Seoul, 2000.
[15] IETF Std. RFC 4050, *Using the Elliptic Curve Signature Algorithm (ECDSA) for XML Digital Signatures*, IETF, S. Blake-Wilson, G. Karlinger, T. Kobayashi, Y. Wang, April 2005.
[16] IETF Std. RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*, IETF, H. Krawczyk, M. Bellare, R. Canetti, February 1997.
[17] Seong-Gyu Sin, “An HMAC Algorithm for Digital Signature,” M. S. dissertation, Catholic Kwandong Graduate School of Education, Gangwon-do, 2003.
[18] Kyung-Sik Kim, “A scheme for improving DHCP and adapting wireless LAN to POSCO,” M. S. dissertation, postech, Gyeongsangbuk-do, 2002.
[19] IETF Std. RFC6704, *Forcerenew Nonce Authentication*, IETF, D. Miles, W. Dec, J. Bristow, R. Maglione, August 2012.

유권정(Kwon-Jeong Yoo)

2015년 2월 : 한밭대학교 정보통신공학과 (정보통신공학 학사)
2015년 3월 ~ 현재 : 한밭대학교 정보통신전문대학원 석사과정
※관심분야 : 네트워크 보안, 컴퓨터 네트워크, 암호화, 시스템 프로그래밍, 임베디드 S/W

김은기(Eun-Gi Kim)

1989년 2월 : 고려대학교 대학원 전자공학과 (전자공학 석사)
1994년 2월 : 고려대학교 대학원 전자공학과 (전자공학 박사)
1995년 2월 ~ 현재 : 한밭대학교 정보통신공학과 교수
※관심분야 : 컴퓨터 네트워크, 임베디드 S/W, 암호화, 네트워크 보안