논문 21-46-04-09 The Journal of Korean Institute of Communications and Information Sciences '21-04 Vol.46 No.04
https://doi.org/10.7840/kics.2021.46.4.651

기업형 무선 네트워크 환경에서의 능동적 Rogue DHCP 공격 영향 분석

노 진 원◆, 박 동 규°

Analysis of the Impact of Active Rogue DHCP Attack in Enterprise Wireless Network Environments

Jin-Won Roh◆, Dong-Kyu Park°

요 약

Wi-Fi 네트워크의 보급은 인간의 삶을 다방면에서 편리하게 하였고, 802.11x 프로토콜이 개선됨에 따라 빠른 통신 속도와 보안성을 보장할 수 있게 되었으나, Wi-Fi의 사용자가 늘어남에 따라 이에 따른 위협 또한 증가하고 있다. 유선네트워크 환경에 비해 무선 네트워크는 물리적인 접근이 용이하여 다양한 위협에 노출되고 있다. 이 같은 위협을 효과적으로 방어하기 위해 기업형 Wi-Fi 보안 환경이 도입되었고, 이는 각각의 사용자에게 서로 다른 암호화를 제공함으로써 Wi-Fi 환경에서의 보안 위협을 방지한다. 본 논문에서는 고도화 된 기업형 Wi-Fi 네트워크 보안 환경에서의 능동적 Rogue DHCP 공격 영향에 대해 분석하였고, 개선된 도구를 개발함으로써 기존 탐지 방법을 우회하는 공격 기법을 제안하였다.

키워드 : 무선네트워크, 802.11, 802.1x, 로그 DHCP, ARP Spoofing, 중간자 공격
Key Words : wireless network, 802.11, 802.1x, EAP, Rogue DHCP, ARP Spoofing, MITM

ABSTRACT

The spread of Wi-Fi networks made human life more convenient in many ways. With the improvement of the 802.11x protocol, it was possible to guarantee faster communication speed and security, but as the number of Wi-Fi users increased, the threat also increased. Compared to the wired network environment, the wireless network is exposed to various threats due to its easier physical access. To effectively defend against such threats, an enterprise-level Wi-Fi security environment was introduced, which prevents security threats in the Wi-Fi environment by providing different encryption to each user. In this paper, the impact of active rogue DHCP attacks in advanced enterprise-level Wi-Fi network environment is analyzed, and the attacking technique is proposed that bypasses the existing detection method by developing an improved tool.

Ⅰ. 서 론

Wi-Fi 네트워크의 보급은 인간의 삶을 다방면에서 편리하게 하였고, 802.11x 프로토콜이 개선됨에 따라 빠른 통신 속도와 보안성을 보장할 수 있게 되었다. IoT 시대의 도래에 따라 차세대 통신 프로토콜이 개발되었으나, Wi-Fi는 여전히 가장 보편적으로 사용되는 무선 네트워크 프로토콜이다. Wi-Fi의 사용자가 늘

◆ First Author : Korea university Department of Software Security, shwlsdnjs@korea.ac.kr, 정회원
° Corresponding Author : Tshinghua University Department of Information Security, dontq0815@gmail.com, 학생회원
논문번호 : 202012-300-B-RN , Received November 30, 2020; Revised January 21, 2021; Accepted January 25, 2021

어남에 따라 이에 따른 위협 또한 증가하고 있다. 유선네트워크 환경에 비해 무선 네트워크는 물리적인 접근이 용이하고, 이를 통해 다양한 악성행위들이 자행되고 있다. 동일한 Wi-Fi 네트워크를 사용하게 되면, 암호화 되지 않은 트래픽은 스니핑 공격에 노출될 수 있으며, OS 취약점 공격 또한 비교적 용이해진다. 이 같은 위협을 효과적으로 방어하기 위해 IEEE 802.1x 보안이 도입되었고, 이는 각각의 사용자에게 서로 다른 암호화를 제공함으로써 Wi-Fi 환경에서의 보안 위협을 방지한다.

본 논문에서는 802.1x의 알고리즘들 중 EAP-TTLS 알고리즘을 소개하고, 해당 환경에서 ARP와 DHCP 프로토콜의 취약점을 이용한 능동적 Rogue DHCP 공격 실험을 진행한다. 개선된 도구의 개발을 통해 기존 방어 기법을 우회하며, 해당 공격 기법을 통해 MITM 공격을 감행하고, 기업 Wi-Fi 환경에서의 공격 영향도를 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 DHCP 프로토콜의 취약점을 이용한 공격 기법과 탐지 및 방어 방법을 살펴보고, 3장에서는 본 논문에서 진행한 공격 실험에 대하여 설명하였다. 4장에서는 실험 결과를 통해 영향도를 분석하고 대응방안을 제시하며, 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 본 론

2.1 관련 연구

DHCP 프로토콜의 기본 동작 과정은 (그림 1)과 같다. 클라이언트가 DHCP Discover 메시지를 보내 새로운 IP주소를 요청하고, 이에 서버가 DHCP Offer 메세지로 새로운 IP를 제시하며, 클라이언트가 이에 대한 응답으로 DHCP Request 메세지를 전송한다.[1] 마지막으로 서버가 DHCP Ack 메시지를 전송함으로써 클라이언트에게 새로운 IP를 할당한다.

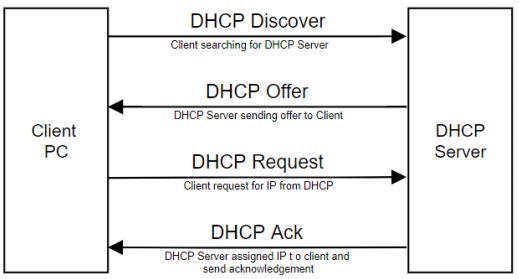

그림 1. DHCP Protocol 동작 과정
Fig. 1. Process of DHCP Protocol

DHCP 프로토콜에는 인증 메커니즘이 존재하지 않는다. DHCP 서버는 새로운 IP를 요청하는 클라이언트에게 어떠한 인증과정 없이 DHCP Offer 메세지를 통해 서버의 IP Pool에 해당하는 새로운 IP를 제공하며, DHCP 클라이언트 또한 가장 먼저 도착한 DHCP Offer 메시지를 참조하여 해당 정보를 적용할 뿐이다. 이러한 특징은 프로토콜의 취약점으로 작용될 수 있다. 해당 취약점을 이용한 대표적인 공격과 방어기법은 다음과 같다.

2.1.1 DHCP starvation attack[2]

DHCP starvation attack은 IP 분배 과정에서 악의적인 클라이언트가 지속적으로 서버에게 새로운 IP를 요청하는 방식의 공격으로, 이러한 요청이 지속됨에 따라 서버가 제공할 수 있는 IP pool내의 IP자원을 고갈시키는 DoS공격이다.

2.1.2 Rogue DHCP[3]

DHCP 클라이언트가 서버로부터 DHCP Offer 메세지를 받아 해당 IP를 적용하는 과정에서 클라이언트는 먼저 도착한 DHCP Offer 메시지에 우선순위를 부여한다. 이를 이용해 악의적인 사용자는 클라이언트가 DHCP Discover 메세지로 새로운 IP를 요청할 때 기존의 서버보다 빨리 DHCP Offer 메시지를 전송함으로써 임의의 IP 주소를 클라이언트에게 할당할 수 있다. DHCP 프로토콜은 IP 주소 이외에도 몇 가지 옵션을 제공하는데 악의적인 사용자는 이 중 Default gateway, DNS Server IP 옵션을 변조해 임의의 목적지로 클라이언트의 트래픽을 유도할 수 있다. 알려진 Rogue DHCP 공격은 두 가지 유형으로 나눌 수 있는데, 클라이언트가 IP를 할당 받기 전 Rogue DHCP 서버를 구축하여 클라이언트의 DHCP Discover 메시지를 기다리는 수동적 Rogue DHCP 공격과 클라이언트가 IP를 할당 받은 후에 클라이언트의 DHCP Discover 요청을 유도하여 임의적인 IP를 할당하는 능동적 Rogue DHCP 공격이다.

2.1.3 ARP Spoofing[4]

ARP란 LAN 환경에서 IP 주소에 따른 MAC 주소를 획득하고 이를 시스템의 ARP table에 적용하는 프로토콜이다 악의적인 사용자는 변조된 ARP패킷을 전송함으로써 ARP 프로토콜을 속이는 것이 가능하고 이를 ARP spoofing으로 통칭한다. 대표적인 공격방법으로 변조된 ARP 응답 패킷을 지속적으로 전송함으로써 대상 시스템의 ARP table을 변조시키는 ARP

poisoning[5]이 있다. 능동적 Rogue DHCP 공격에서는 정상적 ARP 동작과정에서 일어나는 패킷이 아닌 LAN환경에서 IP충돌 시 해당 충돌을 알리는 ARP 패킷을 변조하여 사용하였다.

2.1.4 DHCP Snooping[6]

DHCP 서버가 MAC 테이블을 참조하여 해당 MAC 주소와 포트를 Trusted 와 Untrusted로 나누어 정당한 DHCP 요청을 구분하는 방어기법이다. 유선 네트워크 환경에서는 DHCP 프로토콜 위협을 방지하는 강력한 메커니즘 이지만 무선 네트워크에서는 ARP Spoofing 기법을 통해 이를 우회 할 수 있다.

2.1.5 Cisco Meraki[7]

Rogue DHCP 서버가 DHCP Discover 메시지에 DHCP Discover 메세지로 응답하는 특성을 이용한 방어 기법으로 탐지 에이전트는 일정시간마다 DHCP Discover 메세지를 전송하고 이에 응답하는 정당하지 않은 DHCP 서버를 탐지하고 해당 노드를 차단한다. 이 방어 기법은 Wi-Fi 환경에서도 Rogue DHCP 공격을 효과적으로 방어할 수 있다.

2.2 암호화 및 알고리즘

2.2.1 IEEE 802.1x와 EAP-TTLS

802.1x (Port Base Network Access Control)는 유선LAN의 스위칭 장비에서 포트기반 접근제어를 위한 표준이었으나 무선LAN의 인증 Framework을 제공하기 위해 IEEE 802.11i 표준에 도입되었다. IEEE 802.1x 표준은 크게 세 가지 요소로 구성되며 Supplicant (요청자), Authenticator (인증자), Authentication Server (인증서버) 이다. 요청자는 인증자로부터 인증 요청을 받을 때 클라이언트의 식별정보를 전달하고, 인증자는 요청자의 식별정보를 이용

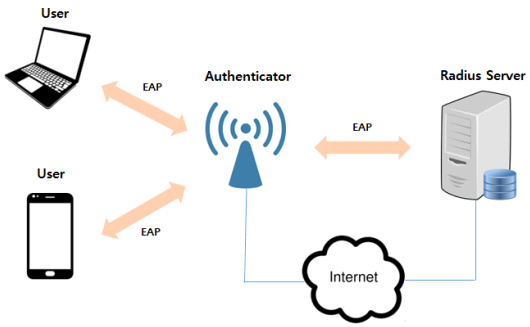

그림 2. Radius Server가 적용 된 802.1x EAP
Fig. 2. 802.1x EAP with Radius Server

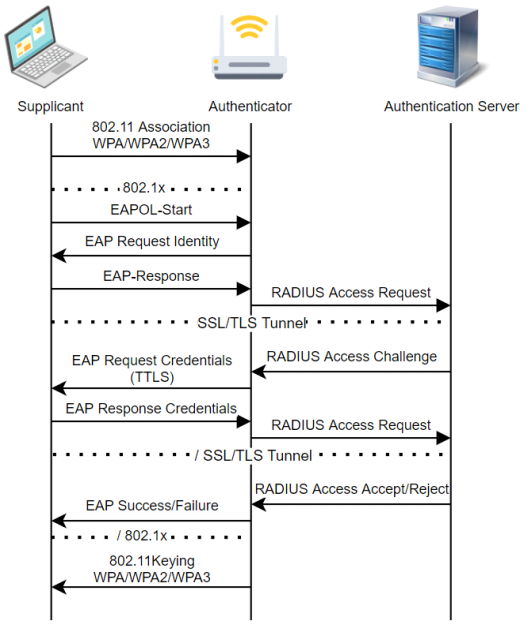

그림 3. EAP-TTLS 인증 프로토콜
Fig. 3. EAP-TTLS authentication protocol

해 인증 서버에게 인증을 요청하며, 결과에 따라 포트를 인증 상태 혹은 비 인증 상태로 나뉜다.

IEEE 802.1x 규격이 제공하는 보안 알고리즘 중 하나인 EAP-TTLS는 EAP-TLS 의 확장된 알고리즘으로 무선 단말 인증은 ID/Password 로 수행하고 서버 인증만 인증서를 이용하는 방식으로 무선 단말에 인증서를 설치할 필요 없이 인증 서버에서 해당 클라이언트에 관한 정보를 이용하여 네트워크 허가를 받을 수 있다. 인증이 완료되면 인증 서버와 무선 단말에 생성되는 세션 키(동적 WEP Key)를 이용하여 암호화 터널이 만들어진다.[8] 해당 인증 프로토콜을 이용한 통신은 외부 공격자의 스니핑 공격에 대한 강력한 보안성을 제공한다.

Ⅲ. 실 험

3.1 실험 개요

3.1.1 능동적 Rogue DHCP와 MITM[9]

기존 연구에서 상용 Wi-Fi AP 환경에서의 능동적 Rogue DHCP 위협은 이미 입증된 바 있다. 802.1x 보안 프로토콜이 적용된 기업형 네트워크 환경에서 능동적 Rogue DHCP 공격의 영향도를 확인하기 위해 실험을 설계하였고, 기존의 방어 기법을 우회할 수 있는 도구를 개발하여 실험을 진행하였다. 공격의 영향

을 받으면 클라이언트의 트래픽이 공격자에게 전달되고, 공격자는 트래픽을 AP로 전달하여, ARP Spoofing 공격을 통해 AP를 속이지 않고도 MITM 공격이 가능하다. 이 때 발생하는 패킷의 수는 일반적으로 ARP Spoofing 공격 시 발생하는 패킷의 수와는 현저한 차이를 보이며, 정상 네트워크 환경에서도 발생 가능한 패킷이 발생되어 기존의 임계치 기반 탐지 방법으로는 탐지가 어렵다. 덧붙여 공격 수행 시에만 Rogue DHCP 서버를 작동하고 공격 후 신속히 서버 작동을 멈추는 방법을 통해 앞서 언급한 Cisco사의 Meraki 시스템에 적용된 탐지 기법을 우회 할 수 있다.

3.1.2 개선점

기존 연구에서 사용된 시험도구는 공격자의 DHCP Sever에 임의의 Default Gateway, DNS Sever 값을 설정한 뒤 변조된 ARP 패킷을 전송함으로써 대상 시스템의 네트워크 환경을 임의의 값으로 변경하는데 그쳤다. 본 연구에서는 해당 도구를 개선하여 Default Gateway 변조 후 실제로 대상 시스템의 패킷을 가로채 해당 내용을 감청할 수 있도록 하였고, 내부적으로 DNS server를 구축하여 실험환경에서 DNS 파밍 공격실험을 실행 후 그 결과를 확인하였다. 나아가 공격 시에만 DHCP server를 작동하게 도구를 설계함으로써 기존의 Meraki 탐지 방법을 우회할 수 있도록 하였다.

3.2 실험 환경

실험 환경 구성은 표 1과 같다.

실험 환경에 쓰이는 AP는 Radius 802.1x 사용자

표 1. 실험 구성 요소
Table 1. components of experiments

Hardware	Description
Laptop	Model: NT900X3N OS: Ubuntu 18.04 Usage: Attacker
Mobile	Model: IPhone XS Max, Galaxy S8 OS: iOS 13, Android 8.0 Oreo Usage: Victim
Wi-Fi Dongle	Model: Wireless PAU09 N600 Chipset: Ralink RT5572
Access Point	Model: Synology MR2200AC Authentication Protocol: EAP-MSCHAPv2, EAP-TTLS, MS-CHAP, PAP or PEAP
Radius Server	Model: Synology DS220j NAS Usage: User Authentication

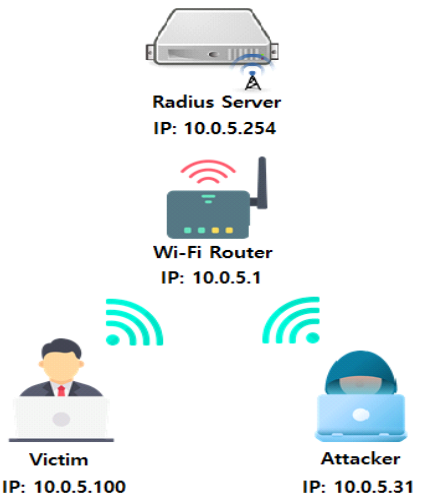

그림 4. Radius 테스트 환경 Topology
Fig. 4. Topology of the Radius environment

인증을 위해 AP 내에 802.1x 구성을 위한 표준 Radius Authentication Server를 지원한다. 본 논문에서는 802.1x EAP-TTLS 보안 프로토콜을 적용하기 위해 Access Point로 Synology 사의 MR2200AC 기기를 이용하였으며, 클라이언트 Device 는 iOS, Android의 모바일 기기를 사용하였다.

802.1x EAP 환경에서 수행되는 실험의 토폴로지 구조는 (그림 5)와 같다. 공격자와 클라이언트는 AP 내 Radius Server를 통해 사용자 인증을 완료하고, 동일한 네트워크에 연결한다. 이 실험으로 기업이나 공공기관, 금융기관 등 고강도의 암호화와 보안 프로토콜이 적용된 환경과 같이 비슷한 환경을 구축하여 실험을 진행하고 결과를 분석함으로써 해당 공격의 영향도를 평가할 수 있다.

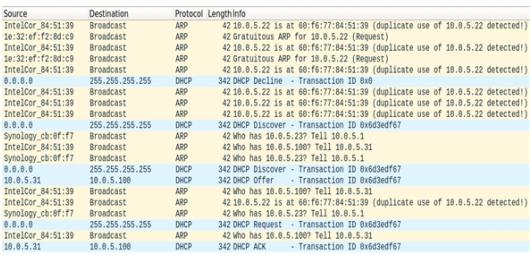

그림 5. DHCP Decline 유도 패킷 전송
Fig. 5. Packet sending to induce DHCP decline

3.3 실험 시나리오

1) 공격자는 스캔을 통해 대상 시스템의 IP를 확인한다.

2) 해당 시스템의 IP의 MAC 주소를 이용해 변조된 ARP 패킷을 생성 후 전송하여 해당 시스템의 IP 충돌을 유발한다. 이 과정에서 Wi-Fi 세션은 유지되며 재인증이 일어나지 않는다.

3) 해당 시스템은 IP 충돌을 감지하고 DHCP decline 메세지를 전송하여 기존 IP의 사용불가를 통보함과 동시에 DHCP Discover 메세지 전송을 통해 DHCP 서버에 새로운 가용 IP를 요청한다.

4) 공격자의 서버가 DHCP Discover에 대한 응답으로 변조된 DHCP Offer 메세지를 전송한다. 이 때 기존의 DHCP 서버의 DHCP Offer 메세지보다 공격자의 메세지가 더 빨리 대상시스템에 도달한다.

5) 대상 시스템은 해당 메세지를 수신 후 DHCP Request를 전송하고 공격자 서버는 DHCP Ack 메세지 전송으로 응답하며 대상 시스템은 인증과정 없이 해당 네트워크 설정 정보를 적용한다.

3.4 실험 및 결과

본 논문에서는 기존 연구에서 입증된 능동적 Rogue DHCP 공격기법을 이용해 클라이언트의 DHCP Decline을 유발하고, 클라이언트가 변조된 Gateway로 전송하는 트래픽을 분석한다.

동일 네트워크 내 클라이언트를 대상으로 실험을 진행하며, 실제로 기업형 네트워크와 동일 수준의 암호화에서의 해당 공격이 미치는 영향에 대해 분석한다.

3.4.1. ARP 전송 공격

일반적인 Wi-Fi 환경에서가 아닌 Radius 서버가 적용된 802.1x EAP 기업형 보안 환경에서 수행했음에도 불구하고 능동적 Rogue DHCP 공격의 영향을 받았으며, IP 충돌을 유도하는 ARP[5] 전송 공격으로 인해 중복 주소로 간주하여 클라이언트의 IP를 무시하고 DHCP Decline을 유도한다.

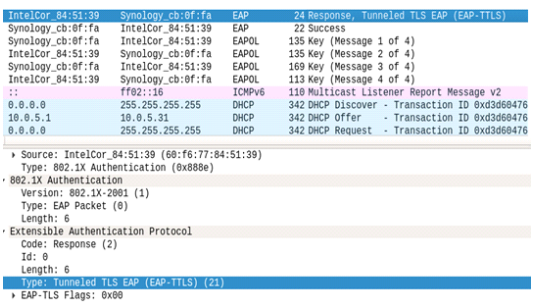

그림 6. 802.1x EAP-TTLS 가 적용된 AP
Fig. 6. Access Point with 802.1x EAP-TTLS

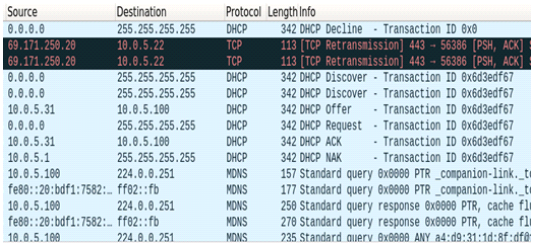

그림 7. Rogue DHCP Server 로부터 IP 재 할당
Fig. 7. IP reassignment from Rogue DHCP Server

클라이언트는 지속적인 공격 데이터 패킷 수신으로 인해 일시적으로 통신이 불가능한 상태가 되고 다시 DHCP Discover 메세지를 브로드캐스트하여 같은 네트워크 내에 있는 DHCP 서버에 IP 주소 업데이트를 요청한다. (그림 7)에 나타난 바와 같이 802.1x의 EAP-TTLS 인증방식을 적용했음에도 불구하고 공격자가 클라이언트로부터 DHCP 요청을 수신하고 변조된 응답 메시지를 전송하였음을 알 수 있다. 주목할 점은 능동적 Rogue DHCP 공격으로 인해 DHCP Decline이 전송 됐음에도 불구하고 인증 프레임 교환 절차를 거치지 않아 공격의 영향을 받는 중 아주 짧은 시간 동안 네트워크 사용이 불가할 뿐, 802.11 Layer 에서는 어떠한 특이사항을 목격하기가 힘들다는 것이다. 공격 수행 이후 DHCP의 IP 분배 과정은 (그림 8)에 나타나 있다.

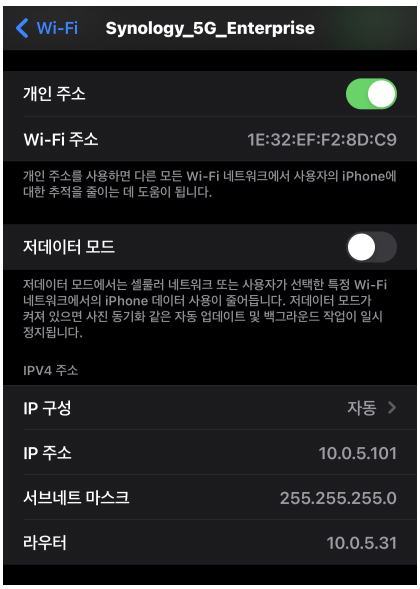

그림 8. 공격 받은 클라이언트
Fig. 8. Attacked Client

3.4.2. 중간자 공격

공격 수행 이후 Gateway와 클라이언트 사이에 송수신 되는 패킷이 공격자에게 전송되도록 중간자 공격 시나리오를 구성하였다. 이후 클라이언트로부터 수신 받는 패킷을 Gateway로 송신하기 위해 포트포워딩 하였고, 외부 인터넷과 연결하기 위해 (그림 10)와 같이 iptables.를 구성하였다.

802.1x/EAP은 각 사용자마다 다른 암호화 키를 사용하고, 전달받은 동적 WEP 세션 키를 이용한 암호화 통신으로 인해 스니핑 공격을 효과적으로 방어할 수 있는데, 능동적 Rogue DHCP 공격을 통해 이를 무력화 시켰으며, 다량의 ARP Spoofing 공격 없이 트래픽 탈취가 가능하다.

전통적 switch 네트워크 환경과는 달리 Wi-Fi 환경에서는 패킷의 변조가 있을 경우 해당 패킷의 실제 발신자를 식별하는 것이 어렵다. 때문에 본 연구에서는 해당 공격의 탐지 및 방어 방안을 네트워크 인프라 측면이 아닌 사용자 시스템 측면에서 제안하고자 한다.

Rogue DHCP 공격의 영향을 받아 Default gateway가 같은 서브네트워크 내의 시스템으로 변경되면 발송된 패킷은 해당 시스템과 기존의 gateway를 거쳐 외부 네트워크로 전달된다. TRACEROUTE 도구를 이용하면 해당 시스템의 패킷 경유지를 추적할 수 있는데, 이를 이용하여 최초 경유지가 동일 서브네트워크인 경우 일반적으로 이를 공격으로 간주하고 탐지 경고 및 해당 Wi-Fi 사용의사를 재확인하는 방법을 제안한다.

iptables_setting

```
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -p udp -j DNAT --to 10.0.5.1
iptables --append FORWARD --in-interface wlp1s0 -j ACCEPT
iptables --table nat --append POSTROUTING --out-interface \
wlp1s0 -j MASQUERADE
```

그림 9. iptables 구성
Fig. 9. iptables configuration

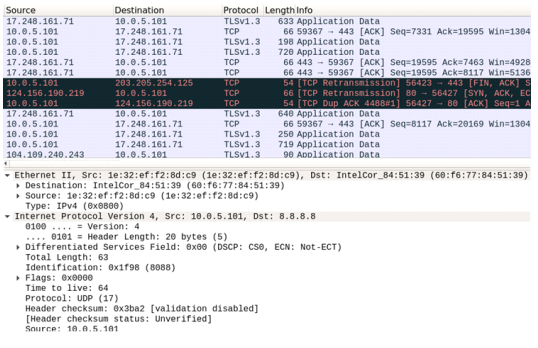

그림 10. 능동적 Rogue DHCP 공격 이후 트래픽 탈취
Fig. 10. Traffic hijacking after active Rogue DHCP attack

Ⅳ. 결 론

본 논문에서는 Radius 인증 서버가 적용된 기업형 네트워크 보안 환경에서의 능동적 Rogue DHCP 공격 영향도를 분석하고 이에 대해 패킷 경로추적을 통한 사용자 시스템 측면에서의 대응 방안을 제시하였다. 실험을 통해 공격이 802.1x/EAP-TTLS 보안 알고리즘을 우회하고 클라이언트를 스니핑 할 수 있음을 확인하였고, 개선된 도구를 개발함으로써 기존 탐지방법을 우회하는 공격 기법을 제안하였다. 제안한 공격 기법은 공격자가 능동적 Rogue DHCP 공격을 수행할 당시에만 DHCP 서버가 동작하도록 하고, 탐지 Agent가 전송하는 DHCP Discover 메세지에 반응하지 않도록 하여 해당 탐지 기법을 우회한다.

References

[1] B. Issac, "Secure ARP and secure DHCP protocols to mitigate security attacks," *Int. J. Netw. Secur.*, vol. 8, no. 2, pp. 107-118, Mar. 2009.

[2] N. Hubballi and N. Tripathi, "A closer look into DHCP starvation attack in wireless networks," *Computers & Secur.*, vol. 65, pp. 387-404, Mar. 2017.

[3] S. Naaz and F. A. Badroo, "Investigating DHCP and DNS protocols using Wireshark," *IOSR-JCE*, vol. 18, no. 3, May-Jun. 2016.

[4] G. Jinhua and X. Kejian, "ARP spoofing detection algorithm using ICMP protocol," in *Proc. ICCCI - 2013*, Coimbatore, INDIA, Jan. 2013.

[5] S. Whalen, *An introduction to arp spoofing*, Apr. 2001, from http://zelja.com/AdminHeaven/misc/security/arp_spoofing_intro.pdf

[6] S. Park, "A rogue AP detection method based on DHCP snooping," *JICS*, vol. 17, no. 3, pp. 11-18, Jun. 2016.

[7] Cisco, *Tracking Down Rogue DHCP Servers*, Oct. 6, 2020, from https://documentation.meraki.com/MX/DHCP/Tracking_Down_Rogue_DHC

P_Servers.
[8] Y.-J. Kim “A complementary plan to vulnerable enterprise WLAN through analysis of security mechanism and threat,” M.S. Thesis, Dept. of Graduate School of Inf. & Telecommun., Konkuk University, 2008.
[9] D. Park, “Practical research of Rogue DHCP attack on Wi-Fi environment,” Tsinghua University, 2019.

노 진 원 (Jin-Won Roh)

2014년 2월 : 한국산업기술대학교 컴퓨터 공학과 졸업
2018년 3월~현재 : 고려대학교 컴퓨터정보통신대학원 소프트웨어보안학과 석사 과정
<관심분야> 컴퓨터 공학, 무선 보안, 네트워크 보안

박 동 규 (Dong-Kyu Park)

2019년 7월 : 중국 Tsinghua University 컴퓨터 공학과 석사
<관심분야> 정보보안, 네트워크 보안, 컴퓨터 공학