

# Wi-Fi AP와 FMC에 대한 무선 호 가로채기 공격 분석 연구

천우성\* · 박대우\* · 장영현\*\*

\*호서대학교 벤처전문대학원 · \*\*배화여자대학

## A Study of Registration Hijacking Attack Analysis for Wi-Fi AP and FMC

Woo-Sung Chun\* · Dea-Woo Park\* · Young-Hyun Chang\*\*

\*Hoseo Graduate School of Venture · \*\*Baewha Women's University

E-mail : deus8522@gmail.com · prof1@paran.com · baewhaoa@paran.com

### 요 약

유선전화에서 무선전화로 전화사용 추세가 전환되면서, 무료 와이파이(Wi-Fi) 기능이 탑재된 휴대폰, 넷북 등 모바일 기기가 빠르게 확산되고 있다. 하지만 무선 인터넷전화는 기존 인터넷망을 이용하여 통화내용을 전달하기 때문에 인터넷서비스가 가지고 있는 취약점이 발생하게 된다. 행정기관에서 사용하고 있는 인터넷전화도 현재 유선에서 무선으로 연결 및 사용률이 증가되고 있다. 본 논문에서는 기존 무선인터넷의 취약점이 발견되는 Wi-Fi AP와 FMC같은 행정기관 인터넷전화 무선 장비에 대한 취약점을 연구를 한다. Wi-Fi AP와 FMC에 대한 취약점을 분석하고, 인터넷전화의 공격에 기본이 되는 호 가로채기 공격실험과 분석을 한다. 보안성이 강화된 인터넷전화를 위한 Wi-Fi AP와 FMC 호 가로채기 공격에 대한 방어와 보안 대책을 연구한다.

### ABSTRACT

Corded telephone to the phone using a wireless phone as the trend to switch, free Wi-Fi-enabled mobile phones, netbooks, and mobile devices, are spreading rapidly. But wireless Internet phone calls using your existing Internet network to deliver Internet services because it has a vulnerability that will occur. Government agencies are using Voice over Internet Protocol(VoIP) calls from the current wired and wireless connection and usage is increasing. In this paper, we have discovered that the vulnerability of wireless internet Wi-Fi AP and the FMC administrative agencies, such as VoIP on your wireless device to study the vulnerability. Wi-Fi AP and the FMC is to analyze the vulnerability. VoIP call interception, attack, attack on the base of the experiment is the analysis. Security-enhanced VoIP call for a Wi-Fi AP and the FMC's defense against man-in-the-middle attacks and is the study of security measures.

### 키워드

Wi-Fi AP, FMC, Registration Hijacking Attack, Attack Analysis

### I. 서 론

최근 스마트폰, 태블릿 PC 등 모바일 기기의 사용이 급속히 확대되면서, 와이파이(Wi-Fi) 기능이 탑재된 스마트폰, 태블릿 PC 등 모바일 기기의 사용이 확산되고 있다. 무선기기들은 무선랜을 이용하여 접속하며, 스마트시대의 확산을 리드하고 있다.

정부에서도 스마트시대에 맞는 행정 서비스를 제공하기 위해 스마트행정의 도입으로, 행정기관

에서 사용하고 있는 인터넷전화도 현재 유선에서 무선으로 연결 및 사용률이 증가되고 있고, 행정기관의 업무도 스마트폰, 태블릿 PC 등 모바일 기기의 사용이 확산되고 있다[1].

Wi-Fi Alliance에 의하면 2015년경에는 스마트폰의 Wi-Fi 탑재율이 90% 넘을 것으로 전망하고 있어, 무선랜 네트워크에서 FMC(Fixed-Mobile Convergence) 서비스는 핵심 인프라로서 예상된다. 따라서 기존 무선인터넷의 취약점이 발견되는

Wi-Fi AP와 FMC같은 행정기관 인터넷전화 무선 장비에 대한 취약점을 연구할 필요가 있다[2].

본 논문에서는 기존 무선인터넷의 취약점이 발견되는 Wi-Fi AP(Access point)와 FMC같은 행정기관 인터넷전화 무선 장비에 대한 취약점을 연구를 한다. 행정기관 인터넷전화 Wi-Fi AP와 FMC에 대한 취약점을 분석하고, 인터넷전화의 공격에 기본이 되는 호 가로채기 공격실험과 분석을 한다. 그리고 보안성이 강화된 인터넷전화를 위한 Wi-Fi AP와 FMC 호 가로채기 공격에 대한 방어와 보안 대책을 연구한다.

## II. 관련연구

### 2.1 무선랜 보안 기술

무선랜 보안기술은 무선 AP에서 설정하도록 하는 기술로 인증과 암호화 방식에 따라 WEP(Wired Equivalent Privacy), WPA(Wi-Fi Protected Access), WPA2(Wi-Fi Protected Access2)로 나뉜다.

각 보안 기술에서 사용자 인증 방법은 사전 공유한 패스워드 입력을 통해 이용자를 인증하는 방법(PSK:Pre-Shared Key)과 별도의 인증 서버를 통해 인증하는 방법이 있다. 암호화 방법은 유선상의 보안성 제공을 목적으로 하는 WEP 방식과 Key 동적 변경, 인증 서버 연동 등 WEP의 취약성을 개선한 WPA와 강력한 블록 암호화 방법인 AES(Advanced Encryption Standard)를 적용한 WPA2 방식이 있다[3].

### 2.2 Wi-Fi 기술

무선랜이란 유선랜(LAN)과 대비되는 표현으로 무선으로 네트워크를 이용할 수 있도록 하는 기술을 통칭하며 국제 표준화 기구인 IEEE에서 802 위원회의 하부그룹인 802.11 그룹에서 표준화를 진행 중이다. 현재까지 제정된 무선랜 관련 주요 표준은 표 1과 같다[4].

표 1. 무선랜 기술표준 및 특징

무선랜 표준	제정 시기	주파수 대역	속도 (최대)
802.11	1997	2.4 GHz	2 Mbps
802.11a	1999	5 GHz	54 Mbps
802.11b	1999	2.4 GHz	11 Mbps
802.11g	2003	2.4 GHz	54 Mbps
802.11n	2009	2.4/5 GHz	540 Mbps

또한 국제 표준 인증 단체인 Wi-Fi Alliance에서는 IEEE에서 제정한 무선랜 표준을 만족하는 장치에 표준적합 인증마크를 부여하고 있다. 대부분의 무선랜 관련장치에는 와이파이 인증마크가 부착되는데 이러한 이유로 흔히 무선랜과

와이파이라는 표현은 혼용되어 사용되고 있다[5].

### 2.4 FMC 개념

FMC(Fixed Mobile Convergence, 유무선통합)는 유선망과 무선망을 융합적으로 구현할 수 있는 기술과 서비스를 의미하며, 최근 스마트폰 보급 확대, 유무선간 수요 대체, Wi-Fi 인프라 확대, 통신시장의 유무선 통합 추세에 따른 경쟁 심화, 기업 모바일오피스 환경 구축 등 다양한 요인으로 인해 확산되고 있는 대표적인 유무선 통합 서비스이다[6].

## III. Wi-Fi AP와 FMC의 공격위협 분석

### 3.1 무선랜(Wi-Fi) 공격위협

무선랜 자체가 가지고 있는 취약점을 사용하여 WarDriving 기술을 사용하여 쉽게 AP의 CID정보와 비밀번호 정보를 확인하여 복제 AP를 설정하여 ARP Spoofing을 할 수 있다.

### 3.2 FMC 서비스 분석과 공격위협

FMC 서비스는 표 2와 같이 주요 통신사업자 추진 주체 및 목적에 따라 유무선통합(FMC, Fixed Mobile Convergence)와 유무선 대체

표 2. FMC/FMS 서비스 특징

구분	유무선통합(FMC)	유무선 대체(FMS)
서비스 개요	· 이동전화에 블루투스 및 와이파이 기능 탑재 · 가정에서의 이동전화 트래픽을 유선망으로 수용하려는 서비스	· 가정 내에서 발생하는 이동전화 트래픽에 대해서 요금할인을 제공 · 유선전화 트래픽을 이동전화 트래픽으로 대체하고자하는 서비스
표준 기술	· UMA기술 (3GPP) · Bluetooth/Wi-Fi · IMS 기반 VCC(3GPP)	· DMA/WCDMA/HSDPA · Femto Cell · Home eNode B(3GPP)
주요 사업자 및 서비스	· 유선통신사업자가 주도 · 브로드밴드와의 번들링 서비스 · BT Fusion, FT Unik 등	· 이동통신사업자가 주도 · 매크로 셀 기반의 홈존 서비스 · Vodafone의 AtHome, USA Hotspot@Home 등
서비스 특징	· 전용 Dual Mode 단말 및 AP (또는 셋탑 박스) 필요	· 기존의 일반 휴대전화 사용 · 주파수 간섭, 유선망 이용대가 산정

(FMS, Fixed Mobile Substitution) 서비스 유형으로 분류한다[7].

FMC 서비스는 듀얼 모드 단말기 하나로 실외에서는 이동통신네트워크를 통해, 실내에서는 유선 전화망이나 IP네트워크를 통해 통화할 수 있는 서비스이며, 이동 전화에 블루투스나 와이파이기능을 추가하여 무선 통화 트래픽을 유선으로 흡수하는 방식이며, FMS 서비스는 주로 이동망을 보유한 이동사업자 주도로 이동망만을 사용하되, 집안 등 특정지역에서 이동통신요금을 유선보다 저렴하게 설정해 유선서비스를 일부를 대체할 수 있어, 기존의 유선전화 트래픽을 이동전화 트래픽으로 대체하고자 하는 서비스이다. 일반적으로 Macrocell이나 Femtocell 장치를 사용하여 특정 지역 내 통화 서비스를 매우 저렴하거나 무료로 제공하며, FMC에 대응하는 개념으로 유선전화 사업자와 경쟁하기 위하여 주로 이동통신 사업자들이 채택한다[8].

FMC 환경은 기존의 이동통신기술, UMA 기술, 유선인터넷기술 등 다양한 기존 유무선 기술들이 통합되는 환경이기 때문에 단일 망에서의 다양한 보안위협들이 상속, 전이, 확대 등 복합적인 형태로 나타날 수가 있다. 다양한 보안 이슈 중 FMC 환경을 구성하는 대표적인 와이파이 및 모바일 VoIP 서비스환경에서의 공격위협을 분석한다.

### 3.3 호 가로채기 공격위협

호 가로채기 위협은 인터넷전화의 등록 정보를 가로채거나 내용을 수정하여 신원을 속임으로써 통화가 불가능하게 만들거나 통화 내용을 가로채어 내용을 확인할 수 있는 위협이다. 무선에서의 취약점을 이용하여 IP와 MAC주소를 알아내고 복제 FMC를 설정하여 공격을 할 수 있다[9].


## IV. 무선 호 가로채기 공격 분석

### 4.1 공격 실험 환경

표 3은 공격 실험 환경에 쓰인 장비의 규격을 나타낸 것이다.

표 3. 주요 장비 규격

MSM310	
	
구분	내용

Access Point MSM301	Type	Indoor Type (Plenum-rated)
	가상서비스 그룹	16개
	듀얼모드 MAP	RF 독립 설계
	암호화	AES 및 RC4
기타	802.3af, L2 isolation, VLAN tagging	
MSM710		
		
구분		내용
Controller MSM710	Number of AP	10
	Maximum Users	2,540
	Current Visitors	100
	구조	Colubris TriPlane
	OS	Colubris
	인증	- RADIUS 인증 및 MS Active Directory 지원 기능 내장 - Captive Portal(Web 인증), MAC 인증 기능 내장
로밍	L2/L3 로밍 (50msec 이내)	

KT에서는 공격탐지 구성도를 구성하여 호 가로채기에 Call Hijacking 공격 시나리오를 작성하였다. 통화시도 시 위변조된 301/302 메시지로 수신자의 통화를 공격자로 돌리는(redirection)공격에서 redirect poison tool 을 이용하여 지속적으로 301/302 메시지를 SIP Server로 송신하여 테스트하고 공격자 PC에서 스크립트를 실행하여 Call-Hijacking 차단 로그를 확인한다.

호 가로채기에 메시지 digest를 실시하여 등록된 단말을 통해 통화 시도를 하고 단말 로그를 통해 등록 시 Authentication과정을 확인하고 MD5 알고리즘으로 동작하는지 여부를 확인한다.

SK브로드밴드에서는 공격탐지 구성도를 구축하여 메시지 Digest 공격으로 등록된 단말을 통해 통화 시도 시나리오를 작성한다.

인증서 변조를 실시하기 위해 등록된 단말에 변조된 인증서로 교체를 시도하고 변조된 인증서를 통해 등록을 시도한다.

4.2 호 가로채기 공격 실시

Wi-Fi Controller를 스캔을 통해 찾아내고 그림 1과 같이 Wi-Fi Controller의 WEP Key를 확인하여 쉽게 접속 할 수 있다.

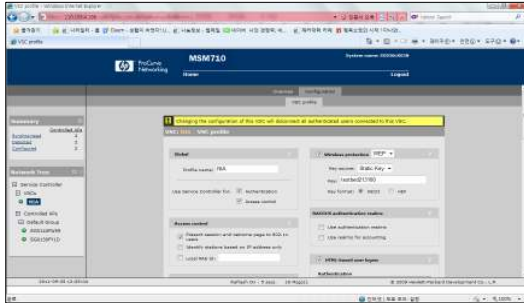


그림 1. Wi-Fi Controller WEP KEY 획득

WarDriving기술을 사용하여 FMC의 정보를 스캔을 통해 그림 2와 같이 스캔된 FMC정보를 사용하여 FMC의 비밀번호를 획득할 수 있다.

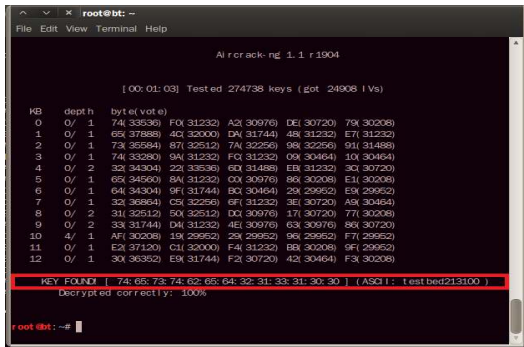


그림 2. FMC 정보 확인

이와 같이 Wi-Fi Controller와 FMC는 무선의 취약점을 가지고 있어 쉽게 비밀번호를 획득하여 관리자 페이지로 접속할 수 있다. 관리자 페이지에 접속하여 정보를 획득할 수 있다. 관리자 페이지에서 IP Phone의 MAC과 IP정보를 획득하여 호 가로채기가 가능하며 그림 3과 같이 암호화 기능이 없는 외부 VoIP Phone과 통화할 때 도청이 가능하다.

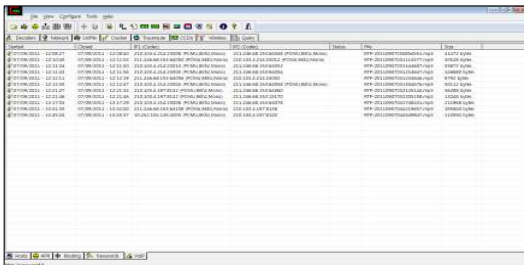


그림 3. 도청 가능 확인

Wi-Fi AP와 FMC의 공격 성공으로 비밀번호 획득 및 관리자 정보를 획득하여 통화에 대해 도청이 가능하여 호 가로채기 공격이 성공을 하였다.

V. 결 론

기존 무선인터넷의 취약점을 가지고 있는 Wi-Fi AP와 같이 FMC에도 똑같이 적용하여 취약점을 발견하였다. 또한, 행정기관 인터넷전화 무선 장비에 대한 취약점도 확인을 하였다.

행정기관 인터넷전화 Wi-Fi AP와 FMC에 대한 취약점을 분석하여 AP의 정보와 FMC의 정보를 확인하였고, 인터넷전화의 공격에 기본이 되는 호 가로채기 공격실험을 하였다. 그리고 보안성이 강화된 인터넷전화를 위한 Wi-Fi AP와 FMC 호 가로채기 공격에 대한 방어와 보안 대책을 연구하였다. 향후 연구로는 무선에서의 취약점을 보완하기 위한 기술의 연구가 필요할 것이다.

참고문헌

- [1] 허원재, "무선 인터넷, 해킹과 전화도청 무방비", 국회 허원재 의원 보도자료, 2009.
- [2] 백종현, "국내 Wi-Fi 보안 현황 및 안전한 무선랜 이용 가이드", TTA Journal No,132, pp. 67-72, Noveber 2010.
- [3] Jin-Young Song, Dea-Woo Park, "A Study on Wi-Fi Hacking Attack using Web," Lecture Notes in Computer Science 6935, ICHIT 2011, September 2011.
- [4] <http://standards.ieee.org/getieee802/802.11.html>
- [5] <http://www.wi-fi.org/brand.php>
- [6] 김환국, 고경희, 윤석웅, 이창용, 김정욱, 정현철, "안전한 FMC 환경 구축을 위한 보안 요구사항 연구", 한국인터넷정보학회, 2010.
- [7] 박호영, 김진기, "유무선 통합(FMC)서비스의 해외 동향 및 확산요인 분석", KT경제연구소, 2009.
- [8] 유승선, 유기형, 임평중, 현철주, 곽훈성, "SIP프로토콜 스택을 기반으로 하는 분산형 IP-PBX 단말기 설계", 한국통신학회논문지, 제 31권 제4호, pp. 377-384, 2006년 4월.
- [9] 박대우, 윤석현, "VoIP 서비스의 도청 공격과 보안에 관한 연구", 한국컴퓨터정보학회논문지, 제11권, 제4호, 155-164쪽, 2006년 9월.