DID 인증기술_Capstone Design

공공 와이파이 해킹 공격 분석 및 보안 방안

• 지도 교수 : 신 승 수
• 학　　과 : 정보보호학과
• 팀　　명 : 하나차이

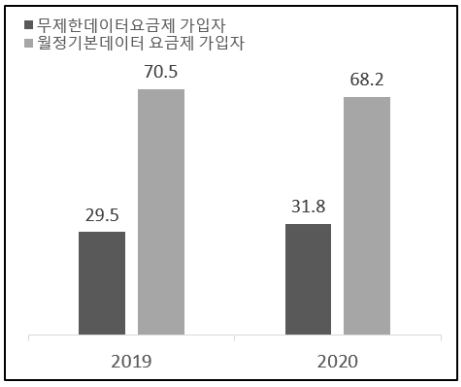
목 차

Ⅰ. 서론

1. 연구배경

현대인에게 인터넷은 필수적인 요소로 자리 잡고 있다. 대부분의 업무나 취미생활이 인터넷을 통해 처리되고 온라인상으로 물건을 주문하거나 금융업무도 수행되고 있다. 또한 스마트폰의 대중화를 통해 무선 통신 장비가 급속도로 증가하였다. 따라서 우리가 생활하는 대부분의 장소에는 무선 공유기가 설치되어 많은 사람들이 와이파이를 사용하고 있다. 하지만 와이파이를 사용하는 사용자들은 보안적인 측면보다는 별도의 이용료 없이 인터넷 서비스를 이용할 수 있는 경제적인 측면을 주로 생각한다[1].

예를 들어 스마트폰 요금제를 무제한 데이터로 사용하게 되면 비용을 과도하게 지불해야 하므로, 무제한 데이터 요금제보다는 저렴한 제한된 데이터 요금제를 선택한 후 와이파이를 필수적으로 사용하는 사람들이 많다는 것이다[2].



[그림 1] 스마트폰 무제한 데이터 요금제 가입자 비율(2019~2020년)

이러한 대중에게 편의를 제공하기 위해 공공 와이파이라는 것이 만들어졌다. 공공 와이파이란 정부, 지자체, 통신사 등에서 제공하는 무선 접속 장치(AP: Access Point)를 이용해 일정 거리 안에서 무선 인터넷을 사용할 수 있는 근거리 통신망 기술을 의미한다. 공공 와이파이의 예로는 버스, 지하철 등에서 무료로 사용할 수 있는 와이파이를 들 수 있다.

공공 와이파이 인프라를 이용해 다양한 네트워크 서비스를 제공할 수 있을 거라 예상했으나, 보안에 취약한 무선 공유기가 급증함에 따라서 이에 대한 보안 공격의 위험성 또한 늘고 있다. 공공 와이파이에 대한 보안 공격이란 악의를 가진 공격자가 무선공유기의 정상적인 작동을 의도적으로 방해하거나, 무선공유기를 통해 송수신 되는 데이터를 엿듣거나 변조하여 피해를 입히는 것을 뜻한다. 근래에는 보안 공격을 손쉽게 실행할 수 있는 오픈 소스(Open Source)가 많이 공개되어, 크래킹(Cracking)에 대한 지식이 없는 사람이라도 사용법을 따라

하기만 하면 막대한 피해를 입힐 수 있는 보안 공격을 실행할 수 있게 되었다[3].

2. 연구목적

무료 와이파이 서비스는 무한대로 확장되고 있으나 공공장소에서 무료로 제공하는 와이파이는 일정 거리 내에서 같은 AP를 사용하기 때문에 다른 사람이 스마트폰에 쉽게 접근할 수 있고 해커들에 의해 악성 프로그램이 설치되어 개인정보 유출 등 각종 사이버 범죄에 노출될 위험이 크다. 공공 와이파이가 실생활에서 많이 사용되는 만큼, 해킹 사례를 분석하고 공격에 대한 탐지 및 보안 방안에 대한 연구가 필요하다고 본다.

본 논문에서는 현재 공공 와이파이에 사용되고 있는 보안 방법에 대해 조사하고, 보안 취약점을 파악하여, 실제 공공 와이파이 환경을 구축해 모의 해킹을 시도하고, 해킹 결과 분석을 통해 공공 와이파이를 사용자들이 안전하게 이용할 수 있는 방법을 모색한다[4].

Ⅱ. 관련연구

본 장에서는 공공 와이파이의 정의에 대해 알아보고, 공공 와이파이에서 사용하는 암호화 방식에 대해 알아본다.

1. 공공 와이파이

공공 와이파이는 정부가 지자체 및 이동통신사와 협조하여 국민들이 자주 이용하는 공공장소에서 와이파이를 제공하는 서비스를 의미한다. 공공 와이파이의 예로는 주민센터, 복지시설, 버스, 지하철, 전통시장 등의 공공장소에서 누구에게나 무료로 제공하는 와이파이를 들 수 있다. 공공 와이파이는 정부가 주체가 된다는 점에서 집, 카페, 영화관 등의 장소에서 개인이나 회사가 직접 설치하여 사용하는 일반 와이파이와는 차이가 있다.

공공 와이파이 설치 장소는 정부부처, 지자체, 통신 사업자 등 관계 기관이 지역 안배, 통신사의 회선 구축 현황, 예산 등을 고려하여 협의를 통해 선정하게 되는데, 주로 서민, 소외계층이 이용하는 공공장소에 설치된다. 공공 와이파이의 가장 큰 장점은 무료로 인터넷에 접속할 수 있다는 점이다. 하지만 AP 기기가 설치 장소 전체를 다 커버할 수는 없고 Wi-Fi 특성상 동시 이용자 수가 많아지면 일시적으로 서비스 품질이 낮아질 수 있어 때때로 접속이 어렵거나 신호가 불안정할 수 있다는 단점이 있다[5].

2. 공공 와이파이 암호화 방식

공공 와이파이 암호화 방식에는 WEP, WPA, WPA2, WPA3가 있다.

가. WEP(Wired Equivalent Privacy)

1999년의 IEEE 802.11무선 LAN 표준에 규정된 WEP(Wired Equivalent Privacy) 암호 방식을 무선 구간에서 전송되는 MAC 프레임들을 40비트 길이의 WEP 공유 비밀 키와 임의로 선택되는 24비트의 Initializtion Vecor(IV)로 조합된 총 64비트의 키를 이용한 RC4 스트림 암호 방식이다[6].

나. WPA(Wi-Fi Protected Access)

TKIP(Temporal Key Integrity Protocol) 및 MIC(Message Integrity Check)를 사용한다. TKIP는 WEP에서 사용했던 RC4 알고리즘을 동일하게 채택하고 향상된 키 관리 방식과 공격자가 접속지점과 클라이언트 사이에 오고 간 패킷(packet)을 수집했거나 변경했는지 판단하기 위한 메시지 무결성 체크 방식이 추가되었다.

다. WPA2(Wi-Fi Protected Access2)

WPA2는 미 정부 보안 요건인 FIPS140-2를 충족하기 위해 128비트의 AES(Advanced Encryption Standard) 알고리즘이 적용되며, CGMP(Computer Cipher Mode With Block Chaining Message Authentication Code Protocol)방식이 기존의 TKIP을 대체한다.

라. WPA3(Wi-Fi Protected Access3)

WPA3는 WPA2의 한계점을 개선하여 향상된 기능을 제공한다. WPA3-개인용(Personal) 모드는 WPA2-개인용 모드와 동일한 암호화 알고리즘과 키 길이를 지원한다. WPA3-기업용(Enterprise) 모드는 암호화 무결성 알고리즘으로 GCMP(Galois/Computer Mode Protocol)를 도입하고 최소 192bit의 키를 사용하여 강화된 암호화 암호화를 제공한다[7].

<표 1> 와이파이 암호화 방식

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	announced by Wi-Fi Alliance
Encryprion	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

3. 공공 와이파이 해킹 공격사례

집이나 사무실은 물론, 카페, 버스, 지하철 등 공공장소에서는 무료로 와이파이를 제공한다. 이러한 장소의 비중은 빠른 속도로 증가하고 있으며, 이에 따라 와이파이 해킹 공격을 시도할 수 있는 지점도 늘어나고 있다. 공격자는 자신의 공유기를 이용해 가짜 와이파이를 생성하여 사용자를 유도할 수 있고, 만약 가짜 와이파이에 접속한다면, 공격자는 사용자가 전송하는 모든 데이터를 확인할 수 있다. 혹은 공공장소에서 사용하는 공유기를 직접 공격할 수도 있다. 관리자 페이지의 인증 ID와 패스워드를 변경하지 않고 기본 값으로 사용한다면 손쉽게 접속하여 공격자는 DNS 변조를 통해 사용자를 피싱 사이트로 유도하거나 사용자의 장치에 악성 프로그램을 유포할 수 있다[8].

혹은 공격자가 공유기를 감염시켜 DDoS 공격에 사용할 수도 있다, 대부분의 와이파이 해킹은 다음과 같은 순서로 이루어진다. 공격자는 대상 와이파이를 지정하고 접근하여 패스워드 크래킹을 시도한다. 성공하게 된다면 공격자는 공유기의 관리자페이지에 접근하여 관리자 권한을 획득한다. 이후 와이파이 사용자들을 피싱 사이트로 유도하거나, 스마트폰, 노트북 등의 장비에 악성 프로그램을 유포해 개인정보를 탈취한다.

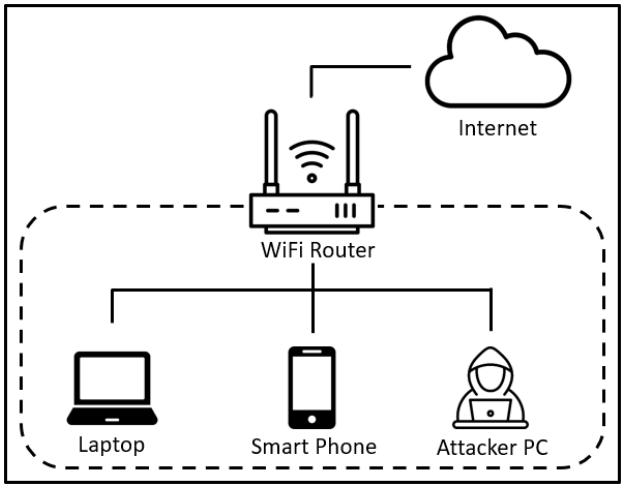
Ⅲ. 공공 와이파이 해킹 공격

본 장에서는 가장 많이 사용되는 공공 와이파이 암호화 방식인 WPA2로 환경을 구성한 후, 공격 시나리오를 작성하여 모의침투를 진행한다.

1. 모의침투 환경 및 시스템 구성

사용자는 버스, 지하철 및 공공장소 등 다양한 장소에서 공공 와이파이에 접속할 수 있다. 노트북, 스마트폰 및 각종 IoT 장비 등 다양한 기기가 공공 와이파이에 접속할 수 있으며, 와이파이를 제공하는 AP를 통해 외부 인터넷을 이용할 수 있다. 한 AP에 불특정한 다수의 사용자가 모이며 이들은 모두 동일한 AP를 사용하기 때문에 기기에 접근이 쉽다.

공격자는 AP에 접속한 무작위 사용자에게 접근할 수 있으며, 정보유출 및 피싱 등의 범죄를 발생시킬 수 있다. 시스템 환경의 전체적인 구성은 [그림 2]와 같다.



[그림 2] 공격 실습 시스템 구성도

실험에 사용된 무선랜은 실습에 사용된 공격용 PC와 USB 포트를 통해 연결되어 있다. 공격용 PC는 AP가 클라이언트와 송·수신하는 암호화된 패킷을 수집하는 역할을 한다. 본 시나리오에서는 WPA2 암호화 방식의 취약점을 이용해 사전 공격을 진행하여 크랙을 진행한다.

<표 2> 모의침투 실험 환경

Classification	Specification
Attack Environment	VmWare, Kali Linux 2022.03
Client(Laptop)	Lenovo IdeaPad 5
Client(Smart Phone)	Apple Iphone 12
WiFi Router(AP)	IpTIME A604MU, WPA2-PSK
Wireless Lan Card	IpTIME N150UA Solo

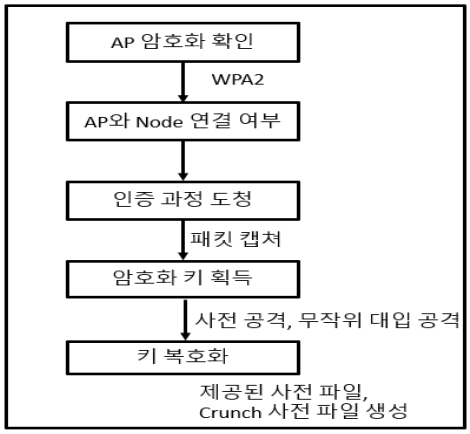
2. 해킹 시나리오

WPA2 해킹 시나리오는 사용자와 AP 사이에 인증 과정(4way-handshake) 중 PSK(Pre-Shared Key)가 포함되어 있다는 점을 이용하여 크래킹을 시도한다.

침투를 시도할 AP의 암호화 방식을 확인한 후, WPA2 방식을 사용 중이라면 다음 과정을 순차적으로 진행한다. 공격자는 AP와 연결되어 있는 무작위 Node(AP와 연결된 기기)를 식별한 후, 연결을 끊기 위해 DoS(Denial of Service) 공격을 시도한다. 이후 연결이 끊어지면 Node는 AP와 다시 연결하기 재인증을 시도하게 한다. 재 인증을 수행할 때, 인증 과정 패킷을 캡처하여 와이파이 패스워드와 ESSID가 결합된 해시값을 탈취한다.

탈취한 값을 이용해 무작위 대입 공격, 사전 공격 등을 통해 와이파이 비밀번호를 크랙 할 수 있다. WPA2 방식은 AES 암호화 알고리즘을 사용하기 때문에 무작위 대입 공격을 통해

크랙 하는 것은 불가능하지만, AP가 취약한 암호를 사용하는 경우 사전 공격에 의해 크랙될 수 있다. 비밀번호 크랙에 성공한다면 공격자는 해당 네트워크에 침투하여 무작위 대상을 상대로 피싱, 도청 및 위·변조 등 다양한 공격을 시도할 수 있다. 전체 크래킹 과정에 대한 흐름도는 [그림 3]과 같다.



[그림 3] 모의 침투 시나리오 흐름도

3. 모의침투

구축한 모의 침투 환경과 해킹 시나리오를 바탕으로 패킷 수집, 사전 공격 수행 준비, 공격 수행 순으로 실제 모의 침투를 진행한다.

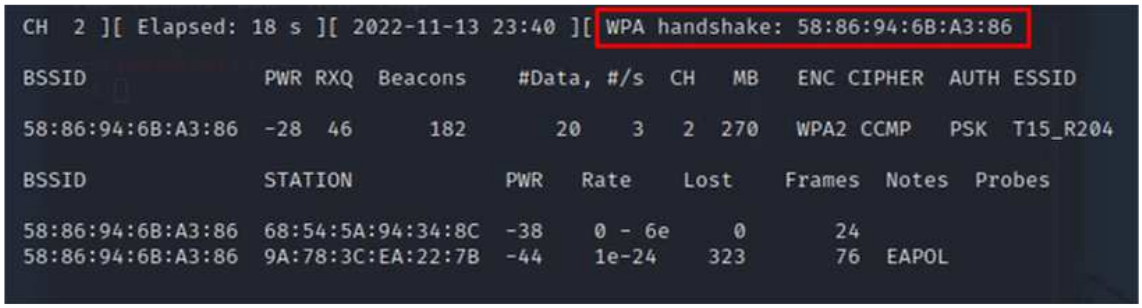
가. 무선랜 탐색

공격용 PC에서 WPA2의 취약점을 공략하기 위해서는 클라이언트가 AP에 접속하는 과정에서 발생하는 4-Way HandShake 패킷을 캡처하여야 한다. 본 연구에서는 칼리 리눅스에서 지원하는 AirCrack-ng 툴을 사용하여 패킷을 수집한다. 목표가 되는 무선랜 AP를 탐색하기 위하여 무선 랜카드를 Monitor 모드로 변경한 후 주변 AP를 모니터링한다.
ESSID로 공격 대상이 되는 AP를 식별한 후 해당 AP의 BSSID 및 패킷을 캡처할 수 있다.

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
12:E3:C7:0B:35:3E	-68	2	0	0	9	720	OPN			T Free WiFi Zone
06:09:B4:74:25:C3	-57	2	0	0	9	720	WPA2	CCMP	MGT	T wifi zone_secure
00:09:B4:74:25:C3	-59	3	0	0	9	720	OPN			T wifi zone
0A:09:B4:74:25:C3	-58	4	0	0	9	720	OPN			T Free WiFi Zone
0A:09:B4:74:25:BB	-71	2	0	0	9	720	OPN			T Free WiFi Zone
58:86:94:6B:A3:86	-37	5	0	0	2	270	WPA2	CCMP	PSK	T15_R204
12:E3:C7:0B:35:52	-72	2	0	0	13	720	OPN			T Free WiFi Zone
06:09:B4:74:25:CB	-80	2	0	0	13	720	WPA2	CCMP	MGT	T wifi zone_secure
02:E3:C7:0B:35:52	-72	3	0	0	13	720	WPA2	CCMP	MGT	T wifi zone_secure
00:09:B4:74:25:CB	-83	2	0	0	13	720	OPN			T wifi zone
10:E3:C7:0B:35:52	-73	3	0	0	13	720	OPN			T wifi zone
00:09:B4:77:C5:8B	-79	0	0	0	5	260	OPN			KT_Free_WiFi
70:5D:CC:D7:E5:C2	-75	8	0	0	4	270	WPA2	CCMP	PSK	T15_1F_R104
88:36:6C:69:EE:9E	-81	2	26	12	4	540	WPA2	CCMP	PSK	1 211-AP

[그림 4] 공격대상 AP 정보 확인

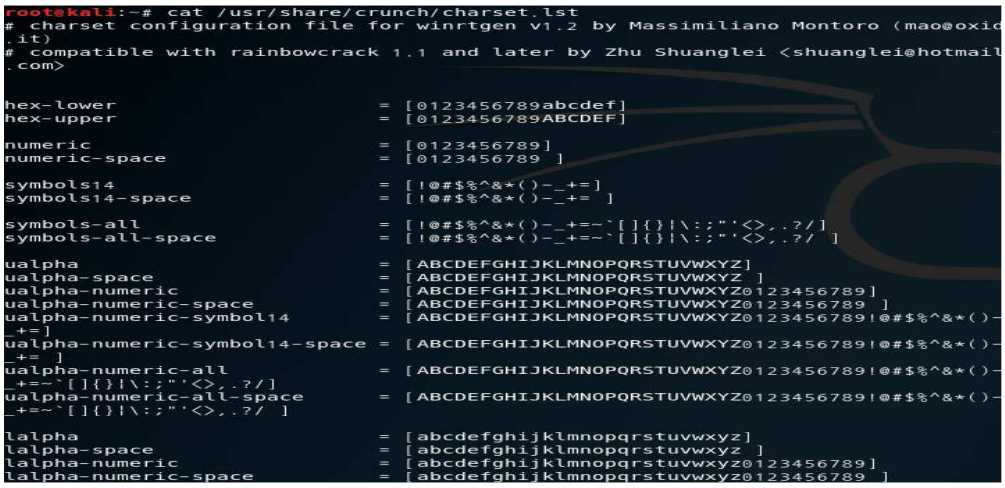
사전 공격을 수행하기 위해서 탐색한 무선랜을 바탕으로 Aircrack 툴을 이용하여 HandShake 패킷 수집할 수 있다.



[그림 5] 수집한 HandShake 패킷

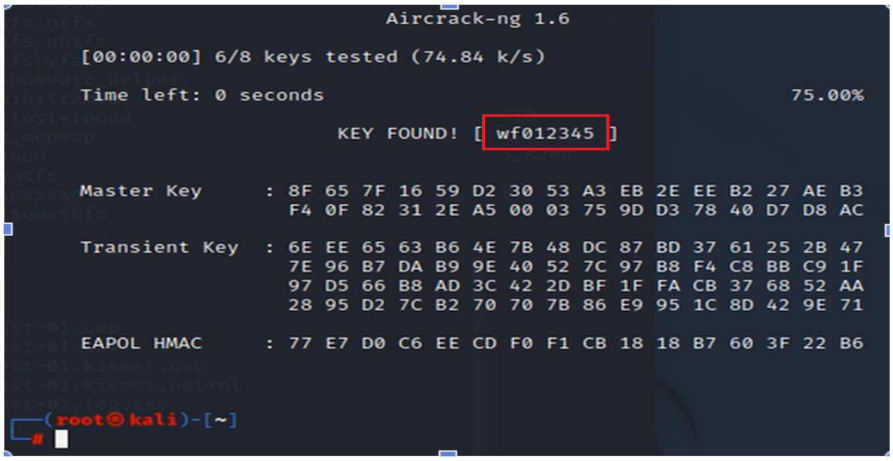
나. 사전 공격

WPA2 암호화 방식의 경우 AES 암호화 알고리즘을 사용하여 무작위 대입 공격에 대한 내성을 가지고 있기 때문에 사전 공격에 의한 크랙을 진행한다. AP가 취약한 패스워드를 사용한다면 사전 공격으로 AP의 패스워드를 크랙 할 수 있다. 본 시나리오에서는 사전 공격을 위한 사전 파일을 칼리 리눅스에서 제공하는 Crunch를 통해 숫자, 영어, 특수문자로 이루어진 키 후보들에 대한 사전 파일을 생성하여 사용한다.



[그림 6] 사전 파일 생성

본문3 [가]에서 진행한 무선랜 탐색 과정에서 획득한 HandShake 패킷 파일에 포함된 PSK 키와 사전 파일을 조합하여 사전 공격을 진행하면 WPA2 암호화 방식에서 사용되는 5개의 매개변수와 조합하여 256비트의 사전 공유 키를 생성한다. 이를 통해 AP의 올바른 패스워드에 대한 추측을 할 수 있으며 사전 파일의 크기에 따라 다량의 시간이 소요된다. 그러나 사전 공격은 무작위 대입 공격보다 경우의 수를 줄일 수 있으며 사전 파일 내에 올바른 암호 값이 포함되어 있다면 패스워드를 크랙 할 수 있다.



[그림 7] 크랙에 성공한 패스워드

사전 공격을 수행할 시, 사전 파일의 크기에 따라 다량의 시간이 소요된다. 시간이 충분하고 '사전 파일' 내에 올바른 암호 값이 포함되어 있다면 4-Way 패킷에서 획득한 WPA2 암호 방식에서 사용되는 5개의 매개변수를 사전 파일로 이용해 [WPA-PSK + SSID]를 조합하여 256비트의 사전 공유 키를 생성한다. 이러한 공유키는 4-Way HandShake 과정에 발생한 매개변수와 결합하여 무결성 검사를 하기 위해 사용되는 PTK(암호화용 임시 키)를 생성하게 되면 이 값을 통해 올바른 AP의 패스워드를 추측할 수 있게 된다.

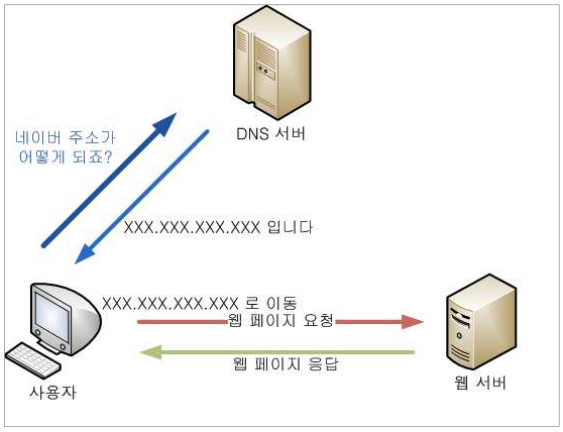
다. 후속 공격

와이파이를 크랙 한 이후 해당 와이파이에 접속하여 공격 가능한 대표적인 방법들에 대해 기술한다.

1. DNS Spoofing

사용자가 인터넷에 접속하기 위해 DNS 서버에 질문을 보낼 때 이를 가로채서 변조된 사이트로 유도하는 일종의 중간자 공격을 의미한다. 공격자는 제작한 피싱 사이트의 웹 서버를 열어놓고 대기하고 있으며, DNS 서버로 전송되는 패킷이 있는지 확인을 한다. 만약 전송되는 패킷을 발견한다면 공격자는 패킷을 전송한 사용자에게 변조된 패킷을 전송한다. 이를 통해 사용자는 전송받은 패킷이 올바른 것이라 믿고 접속을 하며 공격자는 사용자의 정보를 탈취하거나, 지속적인 공격을 위해 악성 프로그램을 설치하는 등의 공격을 가할 수 있다.

실제 공격을 위해 국내의 사용자들이 가장 많이 사용하는 인터넷 포털인 네이버와 외관이 동일한 피싱 사이트를 제작한 후 실습을 진행할 수 있다. 사용자가 네이버에 로그인하기 위해 id, password를 입력하게 되면 이 정보를 공격자가 획득할 수 있으며, 금융 정보 탈취를 위해 인터넷 사기 방지 캠페인과 같은 안내 창을 띄우고 사용자의 입력을 유도할 수 있다.

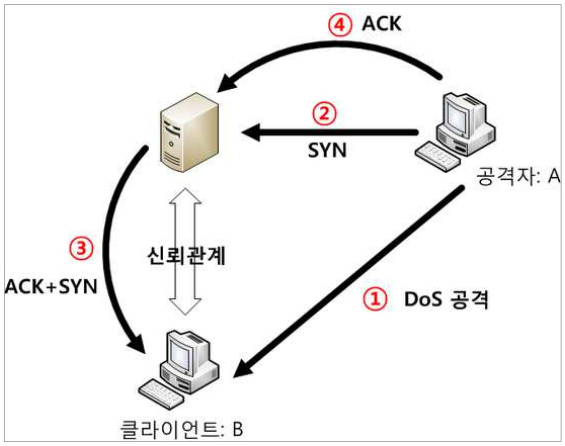


[그림 8] DNS Spoofing

2. ARP Spoofing

사용자가 정상적인 통신을 하고 있는 중에 해커가 중간에 사용자의 통신을 훔쳐서 사용자의 MAC 주소를 같이 사용함으로써 정상적인 통신에 끼어드는 공격이다. 이런 형태는 '중간자 공격'의 형태의 대표적인 공격이다. 공격 절차는 공유기에 연결된 기기들이 일정한 주기로 ARP 패킷을 보내면 해커는 가짜 ARP 패킷을 이보다 짧은 주기로 보낸다.

이때 조작된 ARP 패킷의 양이 더 많기에 AP는 이것에 끌려가게 된다. 공격 대상 AP가 조작된 ARP 패킷의 정보를 따라가게 되면 AP에서 전송하는 모든 정보가 해커의 기기를 거치게 된다. 따라서 전송 정보들이 암호화되어있지 않는 이상 해커가 모든 정보를 볼 수 있다.



[그림 9] ARP Spoofing

Ⅳ. 분석

진행한 모의 침투 실험을 바탕으로 주제인 공공 와이파이에 해킹에 대한 보안 방안을 사용자, 관리자, 국가적 차원으로 구분하여 제안한다.

1. 사용자 차원의 보안방안

사용자들은 공공 와이파이 중 비밀번호가 없는 와이파이는 해킹 가능성이 높기 때문에 사용을 금지하고 신뢰할 수 있는 공공 와이파이만을 사용해야 한다. 또한 공공 와이파이 사용 시 온라인 뱅킹과 같은 민감한 업무를 하게 되면 아이디, 비밀번호, 결제정보 등 각종 개인정보가 노출될 수 있다.

이 경우에 공공 와이파이 대신 데이터를 사용해야 한다. 기존에 연결된 공공 와이파이의 경우 해당 지원범위 내에 들어오게 되면 자동 연결이 되므로 자동 연결 기능을 꺼두거나 와이파이를 사용할 때만 켜는 습관이 필요하다.

2. 관리자 차원의 보안방안

공공 와이파이 공유기 관리자들은 보안에 대한 책임을 갖고 관리자 페이지에서 초기 설정된 비밀번호 대신 추측이 불가능하고 복잡한 긴 비밀번호로 재설정한다. 동일한 비밀번호를 일정 기간 사용하게 되면 보안성이 낮아지므로 주기적으로 변경해준다면 WPA2 크랙에 대한 대비가 가능하다.

오래된 펌웨어를 사용할 경우 이미 알려진 취약점을 이용해 해커가 침투할 확률이 높으므로 정기적으로 공유기 펌웨어 업데이트 여부를 확인하고 새로운 버전의 업데이트가 있으면 적용한다. 무선 침입 방지 시스템인 WIPS 시스템을 사용하여 공격 위협을 사전에 탐지하고 차단해야 한다.

3. 국가적 차원의 보안방안

국가 차원에서 공공 와이파이를 점점 더 확대하고 있다. 하지만 다른 공공 공유기만큼 보안에 취약하여 사용자들의 개인정보 노출 위험이 크다. 이를 개선하기 위해 국가는 국내 보안업체와 협력하여 지금까지 나타났던 무선 랜 해킹 패턴들을 분석한 후 사용자들에게 알려주는 해킹 탐지 서비스를 제공해야 한다.

카카오톡과 같은 사용률이 높은 메신저를 이용하여 사용자에게 최소한의 개인정보에 대한 동의를 구하고, 이 서비스에 대해 제공을 받고자 하는 사용자들이 동의를 누르면 접속하고자 하는 와이파이가 해킹되었는지 즉각적으로 탐지하여 알림을 띄운다. 해킹 위험이 탐지되었을 경우 해당 와이파이에 접속할 수 없도록 차단하고 주변에 있는 다른 안전한 와이파이에 연결할 수 있도록 서비스를 제공한다면 공공 와이파이의 보안성과 신뢰도가 올라갈 것이다.

Ⅴ. 결론

본 논문에서는 공공 와이파이에 사용되는 암호화 방식의 종류와 문제점을 서술하고 공공 와이파이 해킹 공격을 분석하여 보안 방안을 제시하였다.

현대인의 삶에서 인터넷이 필수적인 요소가 되고, 무선 공유기 환경이 범용화 됨에 비해 보안에 대한 인식이 부족하여 와이파이 사용자들은 해킹 위험에 노출되어 있다. 공공 와이파이를 이용하는 대상자 중 일반 사용자가 높은 비율을 차지하고 있기 때문에 금융이나 개인정보가 쉽게 유출되므로 공공 와이파이 공유기 보안이 중요하다.

따라서 이에 대한 방안을 마련하고자 공공 와이파이에 대해 조사한 후, 공공 와이파이 환경을 구축하여 해킹 실습을 진행하였다. WPA2/PSK 암호화 방식에 대해 실습을 진행하였고, Kali Linux의 Aircrack-ng을 이용해 공격을 시도했다. 실습 결과 관리자가 취약한 암호를 설정했을 경우 짧은 시간 내에 쉽게 비밀번호 크랙이 가능했으며, 이는 공격자가 와이파이에 침투한 후, 후속 공격을 가할 수 있다는 의미이다. 후속 공격을 통해 사용자의 패킷을 도청, 위변조하여 정보를 탈취하거나, DDOS 공격에 사용하는 등 다양한 형태로 공격하여 사용자에게 피해를 끼칠 수 있다.

본론의 내용을 바탕으로 사용자, 관리자, 국가적 차원으로 분류하여 대응방안을 마련해 보았으며, 이를 통해 사용자는 공공장소에서 더욱 안전하게 공공 와이파이를 사용할 수 있다.
미래에는 무선랜을 이용하는 장비들이 더욱 많아질 것으로 예상되므로 공공 와이파이를 안전하게 사용할 수 있는 방법에 대한 연구는 필수적이다.

향후 연구로는 최신 암호화 방식인 WPA3에 대한 연구 및 취약점 분석을 진행 한다. WPA3 암호화 방식의 등장으로 보안성을 위해 WPA2에서 WPA3으로 변경되고 있기 때문에 해당 방식의 취약점을 연구하고 대응방안을 마련하여 향후 발생할 수 있는 또 다른 공공 와이파이 보안 문제에 대해 대비할 수 있을 것으로 기대한다.

참고문헌

[1] 이영현, 김기환, 이훈재.(2015).네트워크 취약점을 통한 공유기 공격동향 및 예방방법. 한국정보통신학회, 262-265

[2] 배희라, 김민영, 송수경, 이슬기, 장영현. (2016). 무선공유기 보안공격 분석 및 무료와이파이 해킹 해결방안. 문화기술의 융합, 2(4),65-70.

[3] 정우혁, 이승형. (2016). 무선공유기에 대한 보안공격의 탐지 및 대응. 광운대학교. 87-93.

[4] 조영남, 조정원, 정채은, 강다슬, 장원태. (2018). 공공 와이파이 공격을 통한 취약점 분석 및 보안방안에 관한 연구. 동서대학교. 493-496

[5] “공공 와이파이 서비스 이용안내”, 공공 와이파이, https://www.wififree.kr/pu/si/N01.do.

[6] 국중각, 김희안. “무선 인터넷 서비스를 위한 해킹 대응 방안”, 서비스연구, 제6권 3호, pp.79-90, 2016

[7] 남지현, 이주엽, 권송희, 최형기 “안전한 무선랜 환경을 위한 WPA3 표준의 보안 프로토콜 비교 및 분석,” 한국통신학회논문지, 제44권, 10호, PP. 2,018-2,021, 2019.

[8] https://www.boannews.com/media/view.asp?idx=96130