공공 와이파이 공격을 통한 취약점 분석 및 보안방안에 관한 연구

조영남 · 조정원 · 정채은 · 강다슬 · 장원태*

동서대학교

A Study on Vulnerability Analysis and Security Plan through Public WiFi Attack

Young-nam Cho · Jeong-won Jo · Chae-eun Jeong · Da-seul Kang · Won-tae Jang*

Dongseo University

E-mail : jwtway@gdsu.dongseo.ac.kr

요 약

권고하고 있는 와이파이 통신보안 기술인 ‘WPA2(Wi-Fi Protected Access2)’에서도 취약점이 발견됨에 따라 공공 와이파이를 사용하는 사용자들의 개인 정보도 노출되었다고 볼 수 있다. 본 논문에서는 공격에 의한 공공 와이파이의 보안 취약점을 분석하고, 보안함으로써 사용자들이 안전하게 와이파이를 이용할 수 있도록 하는 방법을 모색하고자 한다.

ABSTRACT

Wi-Fi Protected Access2 (WPA2), a recommended Wi-Fi communication security technology, vulnerabilities are found and Users' personal information may also be exposed. In this paper, we analyze security vulnerabilities of public Wi-Fi by attack and seek to find ways to securely use Wi - Fi by users.

키워드

WAP2, Public Wi-F, Sniffing, ARP Spoofing, ARP

Ⅰ. 서 론

와이파이(Wi-Fi)란, 이더넷(Ethernet) 혹은 유선랜(Wired LAN)이라 부르는 컴퓨터 네트워킹 기술을 무선화한 것이며, 무선 환경에서도 유선 랜과 같은 수준의 속도와 품질로 데이터 통신을 할 수 있도록 한다. 와이파이가 Wi-Fi라는 이름을 갖게 된 것도, 무선(Wireless) 방식으로 유선랜과 같은 뛰어난 품질(Fidelity)을 제공한다는 뜻의 Wireless Fidelity를 줄여서 부르는 말이기도 하다. 이러한 와이파이 인프라를 이용해 다양한 네트워크 서비스를 제공할 수 있을 것으로 예상했으나, 공공 와이파이는 해킹에 취약하다는 것으로 분석되었다. 과학기술정보통신부는 공공 와이파이의 보안 목적으로 와이파이 통신보안 기술인 ‘WPA2(Wi-Fi Protected Access 2)’를 권고하고 있다. 본 논문에서는 현재 와이파이에 사용되고 있는 보안 방법에 대해 조사하고, 보안 취약점을 파악하여 공공 와이파이를 사용자들이 안전하게 이용할 수 있는 방법을 모색한다.

Ⅱ. 무선 암호화 방식

무선 암호화 방식에는 WEP, WPA, WPA2가 있으며, 가장 널리 알려져진 프로토콜들이다.

* corresponding author

표 1. 무선 암호화 방식

방법	WEP	WPA	WPA2
인증	사전 공유된 비밀키 사용	사전에 공유된 비밀키를 사용하거나 별도의 인증 서버를 이용	사전에 공유된 비밀키를 사용하거나 별도의 인증 서버를 이용
암호화	고정 암호키를 사용	암호키 동적 변경	암호기 동적 변형
보완성	노출이 가능하여 사용이 줄음	WEP보단 안전하나 불완전	가장 강력한 보안기능 제공

1. WEP(Wired Equivalent Privacy)

WEP는 데이터 암호화를 위해 RC4 암호를 사용하고, 메시지 인코딩과 디코딩을 위해 40비트 키를 사용하기 때문에 적절히 사용하지 않으면 위험에 쉽게 노출된다. WEP에 사용되는 암호키의 값이 노출되는 경우에 누구나 통신의 내용을 해독해서 볼 수 있으며, 암호키의 값을 모르는 경우에도 널리 알려진 방법을 통해 누구나 데이터의 내용을 해독할 수 있다.

2. WPA(Wi-Fi Protected Access)

핵심 구성요소인 TKIP가 WEP 방식에서 사용된 몇 개의 요소들을 재활용함으로써 펌웨어 업그레이드를 통해 기존 WEP 기기에 설치될 수 있도록 설계되어 있으며 이는 결국 취약점 악용으로 이어졌다. WPA는 WEP와 마찬가지로 침투에 취약하며, 침탈되는 과정은 WPA 알고리즘 자체에 대한 공격과 기기와 접속지점의 연결을 용이하게 해주는 보조시스템인 WPS(Wi-Fi Protected Setup)에 대한 공격을 통해 이루어진다.

3. WPA2(Wi-Fi Protected Access2)

WPA2는 비정부 보안 요건인 FIPS140-2를 충족하기 위해 128비트의 AES(Advanced Encryption Standard) 알고리즘이 적용되며, CCMP(Computer Cipher Mode with Block Chaining Message Authentication Code Protocol) 방식이 기존의 TKIP을 대체한다. WPA 최대 취약점인 WPS 피격위험은 WPA 지원 접속지점에도 그대로 남아있는데, 이를 방지하기 위해서는 WPS 기능이 차단되거나 접속지점 펌웨어를 WPS 지원이 불가능한 기종으로 바꿔서 공격 가능성을 아예 차단해야 한다.

III. 공격 기술

1. 스니핑(Sniffing)

공격 기법 중 첫 번째로는 port mirroring 기법이다. 이 기법은 네트워크 스위치에서 스위치 포트를 통과하는 패킷들을 감시 또는 관찰하기 위하여 패킷들을 다른 스위치 포트를 복사하는 방법이다.

두 번째 공격 기법은 Switch Jamming 기법이다. 이 기법은 스위치가 MAC 주소 테이블을 가득 채우게 되면 모든 포트로 트래픽을 전송하는 특징을 이용한 기법이다. 세 번째 공격 기법은 ICMP[Internet Control Message Protocol, 인터넷 환경에서 오류에 관한 처리를 지원하는 용도로 사용] Redirect 공격이다. ICMP Redirect 공격 방식은 3계층에서 동작되는 스니핑 기법이다. 라우터가 호스트에게 ICMP Redirect 메시지를 보낼 때 공격 대상에게 자신이 라우터이고, 최적의 경로라고 변조된 ICMP Redirect 메시지를 호스트에게 보낸다. 공격 대상은 변조된 메시지를 받고 잘못된 환경을 구축하기 때문에 공격자는 스니핑을 할 수 있게 된다.

2. ARP Spoofing

ARP Spoofing은 로컬 네트워크(LAN)에서 사용하는 ARP 프로토콜의 허점을 이용하여 자신의 MAC(Media Access Control) 주소를 다른 컴퓨터의 MAC인 것처럼 속이는 공격이다. ARP 프로토콜은 인증을 요구하는 프로토콜이 아니기 때문에 간단한 ARP Reply 패킷을 각 호스트에 보내서 쉽게 ARP Cache를 업데이트시킬 수 있다. ARP Spoofing 공격은 ARP Cache 정보를 임의로 바꾼다고 하여 'ARP Cache Poisoning 공격'이라고도 한다.

IV. 공격 시뮬레이션

1. 공격 실험 환경

표 2. 공격 시뮬레이션 실험 환경

서버(PC)	Kali-linux
공격자(PC)	Kali-linux
클라이언트(스마트폰)	GALAXY S8+
	Android 8.0.0(OREO)
공유기(AP)	ipTime N704 BCM

인터넷에 연결된 공유기와 서버 PC는 LAN 선으로 연결이 되어있다. 서버PC에서 공격유무를 지켜보고 공유기 대상으로 주고받아지는 패킷들을 Wireshark를 이용해 관찰할 수 있도록 한다. 공격자 PC는 사용자들과 같은 Wi-Fi 연결을 한다. 일반 사용자들과 달리 공유기에 스니핑, 스푸핑 등 공격을 하여 정보를 빼낸다.

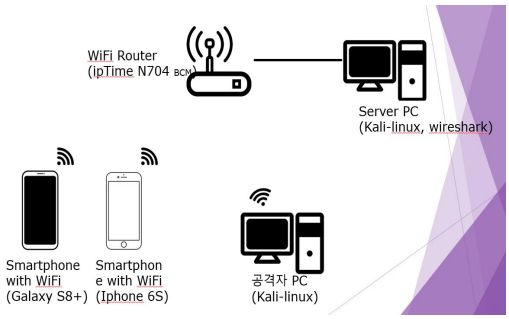

그림 1. 공격 시뮬레이션 시스템 구성도

2. 패킷 분석 Tool

서버 PC에서 공유기IP 기준으로 오가는 패킷을 보기 위해 Wireshark를 사용한다.

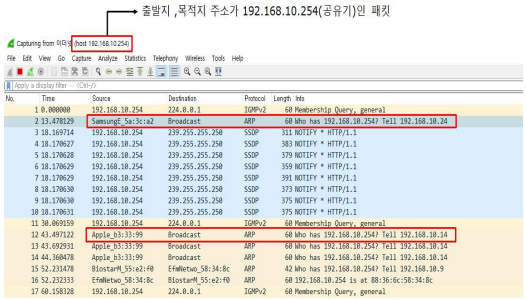

그림 2. Wireshark 실행 화면

서버 PC에서 cmd창에 ipconfig를 하면 기본 게이트웨이 IP로 공유기의 IP를 확인할 수 있다. 실험 환경에서의 공유기 IP는 192.168.10.254임을 알 수 있었다. 클라이언트인 Galaxy S8+, iPhone 6S가 Wi-Fi 접속 시도 시 ARP 패킷을 보내는 것을 확인 할 수 있다.

3. 스니핑 방어대책

스니핑 공격을 방어하는 방법 중 가장 효율적인 방식은 웹서버와 사용자 간에 전송되는 모든 패킷을 암호화하는 방식이다. 패킷이 암호화된 상태에서는 패킷을 중간에서 가로채더라도 암호해독이 불가능하므로 개인정보를 근본적으로 보호할 수 있다.

패킷을 암호화하는 가장 대중적인 방법은 SSL[Secure Sockets Layer, 중요한 데이터를 전송할 때 사용되는 인터넷 통신 규약 프로토콜]과 SSH[Secure Shell, 원격 컴퓨터에 안전하게 액세스하기 위한 유닉스 기반의 명령, 인터페이스 및 프로토콜] 이다. 이러한 프로토콜을 사용하면 모든 패킷이 암호화되어 전송되기 때문에 스피닝 된다 하더라도 해독키 없이 내용파악이 어렵다.

또 다른 대책 방법은 스니퍼 탐지 방법이다. 모든 스니퍼들은 스니핑 공격을 하게 되면 'promiscuous mode'를 설정하여 공격을 실행하는데 이를 관리자가 주기적으로 검사해주면 스니핑을 방지 할 수 있다. promiscuous mode를 탐지 할 수 있는 방법은 ARP를 이용하여 위조된 ARP request를 보냈을 때 ARP response가 오면 상대방 호스트가 promiscuous mode로 설정되어 있는 것이다. 또한 컴퓨터에서 커맨드창에서 ifconfig -a 명령을 이용하여 직접 확인할 수도 있다.

4. ARP Spoofing 공격 방지 대책

ARP Spoofing이 발생하면 네트워크 속도가 저하되거나 정기적인 ARP 패킷이 다량 수신되고, 악성 프로그램의 프로세스가 동작하는 등의 증상이 나타난다. 이러한 증상을 방지하기 위해 시스템과 네트워크 장비에서의 방지 대책을 알아본다.

먼저, 시스템에서의 방지 대책으로는 정적인 ARP table을 관리하여 Gateway의 IP와 MAC 주소를 정적으로 고정시킴으로써 잘못된 ARP Reply 정보가 오더라도 이를 ARP Table에 반영하지 못하도록 해야 한다. 그리고 ARP Spoofing 서버들은 본래의 용도 외에 침입자가 설치한 프로그램으로 인해 네트워크 트래픽 변조 서버로 악용된 것이 대부분이므로, ARP Spoofing 서버로 악용되지 않도록 전체적인 보안수준을 강화하여 공격자에게 악용되지 않도록 관리하여야 한다. 또, 자신의 서버를 안전하게 구축했더라도 공격자는 동인 Subnet 내의 취약한 서버를 해킹하여 트래픽의 도청 및 변조가 가능하므로 아이디, 패스워드, 주민등록번호, 금융정보 등의 데이터에 대한 암호화가 바람직하다. 만약 개인정보나 금융정보가 네트워크를 통해 송수신되는 서버의 경우 SSL(Secure Socket Layey) 방식 등을 이용하여 웹 트래픽을 암호화 시켜야 한다.

네트워크 장비에서의 방지 대책으로는 ARP 패킷을 검사하여 마치 IP 필터링을 하는 방화벽의 동작과 유사하게 지정된 경로로만 ARP 패킷이 전송되도록 하는 기능을 사용하는 것이 효과적이다. 그리고 동일 서브네트워크이지만, 지정된 호스트만 통신을 가능하도록 하는 사설 VLAN 기능을 활용하여 서로 통신할 필요가 없는 서버들을 격리시켜 운용한다면 더 안전한 시스템 운용을 할 수 있다.

V. 결 론

본 논문에서 공공 Wi-Fi의 취약점과 무선 암호화 방식의 종류와 문제점, 다양한 공격을 서술하였다. 무선 공유기 환경이 범용화 됨에 비해 보안에 대한 인식이 부족하여 대다수의 사용자가 해킹에 노출되어 있다. 공공 Wi-Fi를 이용하는 대상자 중

일반 사용자가 높은 비율을 차지하고 있기 때문에 금융이나 개인정보가 쉽게 유출되므로 공유기 보안이 중요하다. 공유기 사용자들은 인증된 와이파이만을 사용하고 안전한 와이파이인지 확인하는 습관을 길러야 하며 개인정보가 필요한 업무는 자제하도록 하는 것이 좋다.

개인정보를 취급하는 앱들은 사용되기 전 알림창을 띄워 사용자들에게 경각심을 일깨워주는 방법도 유용할 것이다. 공유기 관리자들은 보안 수준이 높은 비밀번호를 설정하고 정기적으로 펌웨어를 업데이트한다. 공공 WiFi 공급자는 와이파이 해킹 탐지 서비스를 제공하여 사용자들의 개인 정보가 해커들에 의해 노출되지 않도록 해야 한다.

References

[1] KISA, “2013 Mobile Internet Use Survey,” http://isis.kisa.or.kr

[2] IDC Worldwide Mobile Phone Tracker (2012). Android and iOS- Powered Smartphones Expand Their Share of the Market in the Firs Quarter.

[3] 나성욱, 강경훈, 정종열, “Efficient spread of Wi-Fi Strategy,” 한국통신학회논문지, 2013. 6.

[4] 김현호, Ndibanje Bruce, 장원태, 이훈재, “Domestic Wireless LAN Services Analysis,” 한국정보통신학회, 2014.

[5] Hae-dong Lee, Hyeon-tae Ha, Hyun-chul Baek, Chang-gun Kim, Sang-bok Kim, Efficient Detction and Defence Model against IP Spoofing Attack through Cooperation of Trusted Hosts, 한국정보통신학회논문지 제16권 제12호 (2012년 12월) pp. 2649-2656 2234-4772

[6] 김민욱, “A Study on Detecting Security Threats in Mobile Environment,” 숭실대학원, 2013.12

[7] wiki, “Time to live,” http://ko.wikipedia.org/wiki/Time_to_live

[8] 이해동, Design of Effective Corresponding Model as A Security Policy against Attacks of IP Spoofing in Enterprise Networks, 경상대학교, 2013.2

[9] 신동명, 신동호, 고경희, “A Study on the Detection Method of Wireless Rogue Access Pointm” 인터넷정보학회 학술발표대회 논문집, Vol. 5, No. 2, 2004. 11.

[10] S. H. Hong and Y. J. Seo, “Countermeasure of Sniffing Attack: Survey,” *Journal of Convergence for Information Technology*, Vol. 6, No. 2, pp. 31-36, 2016.

[11] J. H. Soo and G. S. Chae, “Detection of Forgery of Mobile App and Study on Countermeasure,” *Journal of Convergence for Small and Medium Business*, Vol. 5.