스마트폰 상에서 무선 네트워크 보안 문제점 분석

김기환*, 이영실*, 이훈재*

*동서대학교

An Analysis of Security Problem against Wireless Network in Smartphone

Ki-Hawn Kim*, Young Sil Lee*, HoonJae Lee*

*Dongseo University

e-mail : ghksdl90@naver.com, youngsil.lee0113@gmail.com, hjlee@dongseo.ac.kr

요 약

통신기술이 발달하면서 스마트폰에서의 다양한 응용 프로그램(파일 관리, 게임 등) 앱을 실현할 수 있는 환경이 조성되었고, 스마트폰을 통해 기존의 PC, 노트북, 태블릿 PC 등이 수행하였던 주요 업무 처리를 할 수 있어 사용자의 편의성을 높여주고 있다. 이때, 3G, 4G 등의 데이터 통신을 이용할 경우 전송되는 데이터양에 따른 추가 비용이 발생하게 되므로, 사용자들은 무선 네트워크를 사용하여 인터넷에 접속하는 것을 선호한다. 그러나 무선 네트워크를 이용할 경우 외부에서 손쉽게 정보를 탈취하거나 변조, 또는 인가되지 않은 무선 접속장치(AP)를 통한 중간자 공격으로 사용자의 스마트폰 내에 저장된 개인정보에 접근하는 등 다양한 공격 가능성이 존재한다. 이에 본 논문에서는 먼저, 스마트폰에서 무선 네트워크 사용 시 발생 가능한 보안 문제점에 대하여 분석하고, 인가되지 않은 무선 접속장치(AP)를 탐지할 수 있는 방법에 대하여 살펴본다. 또한, 이를 통해 보완하여 보안성을 강화할 수 있는 방법에 대하여 고찰한다.

ABSTRACT

Due to the development of communication technology, a conventional major business through PC, laptop or Tablet PC can be performed via a smartphone and it is increasing the user's convenience. At this point, the user prefers to connect to the Internet using the wireless network because it occurs an additional charge according to the amount of data to be transmitted when using a data communication through 3G or 4G. However, when using a wireless network, there is a possibility of several attacks such as easily steal or modulate the information from the outside or to gain access to personal information stored in the user's smartphone with man-in-the-middle attacks by using the fake AP. IIn this paper, we describe how you can detect the AP when you use LAN of the smartphone, were analyzed for this vulnerability, has not been approved. Furthermore, Also, we discuss ways which can enhance the security when user the access to the internet services (i.e., internet, public/private cloud service, etc.) via wireless network in smartphone.

키워드

무선 접속장치(AP), 무선 네트워크 보안 문제점, 스마트폰

Ⅰ. 서 론

스마트폰은 사용자가 원하는 앱(APP, Application의 줄임말)이란 응용 프로그램을 설치하여 통신망을 통한 각종 정보의 수집 및 활동 등을 할 수 있다는 점에서 기존의 휴대전화와 다른 독특한 특징을 가지고 있다. 이러한 스마트폰의 기능은 통신규격의 발달로 인해 가능했는데, 2002년에 등장한 3G(3세대 이동통신기술)가 가능해지면서 동영상 등을 빠른 속도로 전송받을 수 있게 되었고 최근에는 4G(4세대 이동통신기술)로 발전하면서 등장한 'LTE', '와이브로'와 같은 고속전송 데이터 통신이 가능한 이동통신 규격 역시 소비자의 스마트폰 활용을 더욱 증진시키고 있다. 또한, 통신기술이 발달하면서 스마트폰에서의 다양한 응용 프로그램(파일 관리, 게임 등) 앱을 실현할 수 있는 환경이 조성되었고, 스마트폰을 통해 기존의 PC, 노트북, 넷북 등이 수행하였던 주요 업무 처리를 할 수 있어 사용자의 편의성을 높여주고 있다[1].

그러나, 저장 공간의 제약과 분실 혹은 도난에 따른 금융업무와 관련된 정보가 유출, 도난을 통해 입수한 모바일 단말기의 전화부를 통해 사용자임을 사칭하여 2차 피해를 불러오는 사례가 최근 빈번히 발생하고 있다. 또한, 사용자가 3G, 4G 등의 데이터 통신을 이용할 경우 발생하는 추

가 비용을 줄이기 위하여 무선 네트워크를 사용하여 인터넷에 접속하는 경우가 많으나, 무선 네트워크의 경우 공격자가 해당 무선 접속장치의 비밀번호를 알아내고 동일한 환경을 만들어 낼 수 있다. 따라서 사용자가 자주 사용하는 무선 접속장치와 동일한 가짜 무선 접속장치를 만들고 더 강한 전파를 송신하여 신호강도를 우선순위로 하는 정책을 악용하게 될 경우 사용자 모르게 접속하도록 유도할 수 있다.

이에 본 논문에서는 먼저, 무선 접속장치(AP)의 개방적인 사용으로 인해 발생할 수 있는 보안 취약성에 대하여 살펴보고, 모바일 단말기를 대상으로 다양한 실험을 통해 이를 확인한다. 또한 결론을 통해 이러한 문제점을 해결할 수 있는 방안에 대하여 고찰한다.

Ⅱ. 스마트폰 상에서 무선 네트워크

최근 사용되고 있는 스마트폰에서의 무선접속 환경은 크게 두 가지로, 먼저 이동통신 표준 기술인 3G(3세대 이동통신망) 또는 4G(4세대 이동통신) 환경과 와이파이 얼라이언스(Wi-Fi alliance)의 상표명으로 IEEE 802.11 기반의 무선랜 연결과 장치 간 연결 등의 기술을 지원하는 Wi-Fi 연결 환경으로 나누어 볼 수 있다. 이 중 Wi-Fi(Wireless Fidelity)는 보통 Wireless LAN이라 불리며, 무선 접속장치 등 무선 접속장치(AP, Access Point)가 설치된 곳에서 전파나 적외선 전송방식을 이용하여 일정 거리 안에서 무선 인터넷을 할 수 있는 근거리 통신망을 칭하는 기술이다. 아래의 그림 1은 3G와 Wi-Fi의 무선 인터넷 망 범위를 간략하게 표현한 그림이다[2].

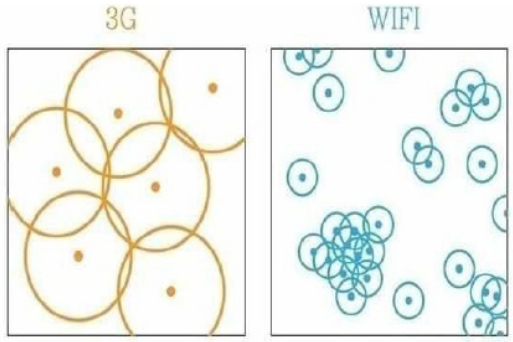

그림 1. 3G와 Wi-Fi의 무선인터넷 망 범위[2]

3G망은 거의 모든 지역에서 사용할 수 있으나 데이터 전송 속도가 느리고, 4G의 경우 정지 시에는 최대 1Gbps, 이동시에는 100Mbps이상의 빠른 전송 속도로 3G와 비교했을 경우 50배 이상 빠른 속도를 제공하고 있다. 그러나 4G를 이용할 경우 데이터 전송량에 따른 추가 비용이 발생하게 되므로, 스마트폰 사용자들은 무선 데이터 요금을 아끼기 위하여 무작위로 검색된 무선 접속장치(AP)를 이용하는 등 공중 무선 네트워크나 사설 무선 네트워크를 통해 접속하는 빈도가 더 높다.

그러나 보안을 설정하지 않은 무선 네트워크의 경우 외부인이 무선 접속장치(AP)를 무단으로 사용할 수 있다. 만약 공격자가 악의적인 의도를 가지고 악성코드를 심어놓은 무선 접속장치(AP)에 접속할 경우, 스마트폰 사용자가 인지하지도 못한 상태에서 이러한 무선 접속장치(AP)에 접속하는 것만으로도 악성코드에 감염될 수 있다. 그 외에도 스푸핑(Spoofing)과 스니핑(Sniffing), 서비스 거부 공격(DoS) 등 다양한 해킹 기법을 통해 보안 사고를 유발시킬 수 있으며, 유출된 정보를 통한 2차 피해 역시 발생할 수 있다.

Ⅲ. 무선 네트워크 보안 문제점

Wi-Fi는 무선으로 연결을 성립하기 때문에 무선 접속장치가 설치된 위치를 확인하는 것이 어렵고 원거리에서 신호강도와 이름 비밀번호만을 통해 접속이 이루어지므로 안전성을 평가하기에는 어려운 점이 있다. 또한 가정과 사무실에서도 무선 접속장치를 사용하고 있지만 대부분의 무선 접속장치는 초기 설정으로 방치하여 사용하는 사용되고 있다. 따라서 공격자에게 충분한 시간과 정보만 주어진다면 공공장소뿐만 아니라 가정과 기업의 Wi-Fi도 위험성이 높다고 볼 수 있다.

3.1 가짜 무선 접속장치(AP)를 통한 중간자 공격의 위험성

가짜 무선 접속장치를 활용한 무선 네트워크 보안 위협 요소 가운데 Honey pot AP와 AP MAC Spoofing을 통하여 접속된 사용자의 ID, 패스워드를 유출하거나 금융정보 및 개인정보 유출을 통한 보안 위험성이 존재한다.[3]

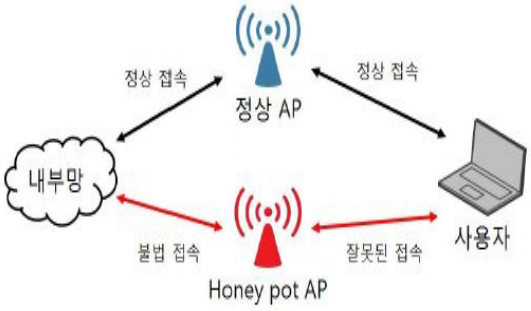

그림 2. Honey pot AP, AP MAC Spoofing 구성도[3]

또한, 중간자 공격 기법 가운데 Evil Twin 공격

(Wi-Fi 피싱)의 경우 로그온한 사람들을 속이고 비밀번호나 신용카드 등의 개인정보를 탈취하기 위해 합법적인 네트워크인 것을 가장한 무선 네트워크를 가리키는 것으로 공격자가 합법적인 무선 네트워크 제공자임을 가장하여 스마트폰이나 휴대 전화로 핫스팟에 연결한 무선 사용자들을 공격한다. 하지만 보안이 필요로 하는 장소에서는 WIPS(Wireless Information Protection System)를 통하여 자신을 제외한 나머지 무선 접속장치의 접근을 통제하는 것으로 불법적인 무선 접속장치의 접근을 차단하면 된다. 하지만 대부분의 무선 접속장치는 가정과 공공장소에 설치되어 있기 때문에 좁은 법위에 다수의 무선 접속장치가 설치될 가능성이 높아 적합하지 못하다. 또한 건물 밖의 환경의 경우 위험에 쉽게 노출 될 수 있다. 이와 같은 환경은 인위적으로 조작될 위험성이 높아 가급적 사용을 자제하는 방법밖에 없다.

3.2 저장된 무선 접속장치(AP) 접속 구별

단말기를 통하여 성공적으로 접속이 완료된 무선 접속장치와 관련된 정보는 단말기 내부에 저장하여 다음 접속 시도의 소요시간을 단축시켜준다. 하지만 암호화된 무선 접속장치는 항상 동작하고 있기 때문에 쉽게 모방될 수 있다. 공격자가 공격을 대상으로 무선 접속장치와 같은 환경을 구축한다면 동일한 이름과 더 높은 신호 강도를 통해 접속을 유도할 것이다. 만약 적외선 센서를 통한 연결도 힘들다면 이전의 저장된 정보를 이용하여 구별하는 방법이 존재한다. 무선 접속장치는 안정적인 전력과 유선 통신망이라는 제한된 조건 때문에 설치 환경이 유지되는 조건을 이용해 짧은 네트워크 경로 구조를 해쉬 암호화 과정을 통해 네트워크 구조가 유출되지 않고 비교하여 확인이 가능하다.

Ⅳ. 실험을 통한 가짜 무선 접속장치(AP) 식별

지금까지 무선 접속장치의 신분을 증명하는 내용을 정리하면 다음과 같다. 첫째 무선 접속장치는 사설 네트워크로 분류되기 때문에 C 클래스 주소를 가진다. 둘째 물리적인 설치조건 때문에 위치를 변경하지 않고 사용한다. 셋째 제한된 인원만이 사용하기를 원한다. 이에 본 장에서는 모바일 단말기를 대상으로 정상적인 네트워크 환경과 노트북을 이용한 가짜 무선 접속장치(AP) 연결에 따른 통신 결과를 살펴본다.

4.1 환경에 따른 네트워크 경로 변화

흔히 사용되고 있는 무선 접속장치는 주소를 생성하고 할당하는 기능이 기본적으로 제공되기 때문에 소요되는 시간이 높지 않다. 또한 한 개의 주소를 여러 개의 주소로 변환하기 때문에 사설 네트워크 규칙에 따라 192.168.xxx.xxx 형식의 구조를 취하게 된다. 아래의 그림3은 정상적인 무선 접속장치에 연결을 시도할 경우의 네트워크 주소를 나타내며, 정상적인 무선 접속장치는 위의 조건을 충족함을 알 수 있다.

```
traceroute to yahoo.com (98.139.183.24), 30 hops max, 38 byte pack
ets
 1  192.168.10.2 (192.168.10.2)  1.740 ms  2.899 ms  0.854 ms
 2  192.168.112.254 (192.168.112.254)  5.859 ms  6.225 ms  4.638 m
s
 3  192.168.111.1 (192.168.111.1)  1.892 ms  4.303 ms  7.355 ms
```

그림 3. 원본 무선 접속장치(AP) 연결 시

그러나 만약 공격자가 추가적인 비용을 지불하지 않고 단지 노트북을 통해 무선 접속장치 환경을 구축한다면, 그림 4와 같이 정상적인 네트워크보다 추가적인 시간이 소모된다. 또한 변환 소요시간 때문에 알 수 없는 네트워크 구간이 생긴다.

```
traceroute to yahoo.com (98.138.253.109), 30 hops max, 38 byte pac
kets
 1  192.168.137.1 (192.168.137.1)  4.456 ms  *  17.212 ms
 2  *  *  *
 3  192.168.10.2 (192.168.10.2)  13.061 ms  5.036 ms  4.821 ms
 4  192.168.112.254 (192.168.112.254)  5.646 ms  5.706 ms  7.141 m
s
```

그림 4. 가짜 무선 접속장치(AP) 경유 시

또한, 공격자가 비정상 적인 네트워크 경로 구별을 통해 구별하는 상황을 피해 이동통신망을 거쳐 인터넷에 연결되는 구조를 만든다면, 아래의 그림 5와 같이 C 클래스 주소에서 곧바로 B 클래스 영역으로 변경되는 것을 확인할 수 있다.

```
traceroute to yahoo.com (206.190.36.45), 30 hops max, 38 byte packets
 1  192.168.43.1 (192.168.43.1)  5.066 ms  3.327 ms  2.197 ms
 2  110.70.139.233 (110.70.139.233)  45.319 ms  72.876 ms  33.416 ms
 3  110.70.139.154 (110.70.139.154)  83.283 ms  57.892 ms  37.262 ms
```

그림 5. 이동통신망 연결된 와이파이

4.2 네트워크 경로 식별

무선 접속장치의 경우 사설 네트워크 주소 사용으로 인한 주소 고정, 전력 공급과 유선 인터넷 길이 제약사항, 무선 네트워크 설치 후 위치 변경이 이루어지지 않는 점 등의 문제가 발생할 수 있다. 이를 해결할 수 있는 한 가지 방법으로, 기

존에 접속이 이루어진 정상적인 네트워크에서 공인된 기관까지의 경로를 해쉬 암호화를 통하여 모바일 단말기에 등록한다면, 이후 모방된 무선 접속장치와의 연결이 시도될 경우 해쉬 값을 비교함으로써 구별이 가능하다. 이때 인터넷 구간은 경로가 변경될 수 있기 때문에 사설 네트워크 범위까지를 비교하는 것으로 사용될 것이다.

Ⅴ. 결론

통신기술의 발달로 인해 스마트폰의 시대가 도래하였으며, 2008년 이후로 전 국민의 절반 이상이 스마트폰을 사용하고 있다. 이러한 스마트폰으로 인해 언제 어디서든지 웹 서핑과 앱(App) 사용을 통한 업무 또는 취미생활이 가능해졌다. 그러나 스마트폰 자체의 보안문제인 악성코드 감염, 사용자 ID 도용, 스마트폰 내부에 저장된 문서, 이메일 등의 해킹 및 도청, 폰 분실로 인한 개인정보 유출 등 다양한 보안 문제점 역시 대두되고 있다. 또한 데이터 통신 시 추가적으로 발생하는 비용을 줄이기 위해 사용자들이 주로 무선 네트워크를 이용하여 인터넷에 접속하거나 영화, 게임 등 다양한 자료를 다운받게 되는데, 이때 특수한 장비를 이용해 SMS, 음성 및 기타 데이터를 도청 및 감청하는 방법 등 다양한 보안 문제점을 가지게 된다.

한 가지 예로, 안드로이드 앱 중 Dsploit의 경우 관리자 권한 획득과 블랙마켓을 통하여 설치와 사용이 가능하며, 동일한 Wi-Fi에 접속한 모든 사용자들을 대상으로 공격이 가능하다. 이때 사용자가 웹을 통해 로그인이 된 경우 해당 로그인 세션을 가로채는 것으로 공격자는 아이디와 비밀번호 없이 접속이 가능하다. 이와 같은 공격으로 사용자의 계정에 접근하여, 패스워드, 파일, 이메일 계정 정보, 신용카드 정보, 은행 계좌 등과 같은 개인 정보들을 해킹 당하게 되며, 탈취된 전화부에 등록된 지인들에게 악성프로그램이 포함된 메일을 보내는 등 2차 피해를 유발할 수 있다. 이러한 점을 보강하기 위해 무선 네트워크 이용 시 전송되는 데이터를 암호화하여 전송하도록 규정하고 있으나, 이 경우 암호화하는 추가 데이터양이 증가하게 되며, 서비스의 제공 속도에도 영향을 미치게 되어 금전적인 손실이 발생하게 된다. 따라서 은행권과 같은 높은 수준의 암호화 과정을 사용하지는 않는 것이 현실이다.

본 논문에서는 무선 접속장치를 통한 사용자 정보 보안문제가 발생할 수 있는 사례를 살펴보고 어떤 정보도 공개되지 않은 무선 접속장치를 어떻게 인증하고 이미 저장된 접속장치는 어떻게 확인할 것인가를 살펴보았다.

앞서 언급한 바와 같이 무선 접속장치는 설치 제약 조건이 까다롭고 이동이 불가능하기 때문에 네트워크 구조의 변화가 없다. 이러한 점을 활용하여 일방향 암호 알고리즘을 사용한 암호화를 통해 네트워크 구조를 유출하지 않고 이전의 연결을 시도하였던 무선 접속장치가 맞는지 확인이 가능하다. 그러나 현재 사용되고 있는 무선 접속장치의 경우, 단일 매체만을 통한 통신이 이루어지고 있는 실정이다. 통신수단 사용의 증가에 따른 개인정보 유출문제에 대비하기 위해서는 사용자의 개인 무선 접속장치(AP)에 WEP(Wired Equivalency Privacy) 또는 WAP(Wi-Fi 보호 접속)을 사용하여 무선 네트워크의 연결을 암호로 보호하여 인가되지 않은 사용자의 접속을 차단하거나, 공공장소에서 접속하기 전 무선 접속장치(AP)를 확인하는 등 사용자의 적극적인 노력과 더불어 무선 접속장치 신호의 검증 수단을 늘려 이를 검증하는 노력이 필요하다.

참고문헌

[1] 김한가희, 이지헌, “스마트폰 클라우드 서비스에서의 개인정보 침해 유형 및 관계 법령에 대한 소고,” 연세대학교 법학연구 23권 1호, 2013년.

[2] 임성수, 송준영, 김봉현, 조동욱, “스마트폰과 무선 공유기의 거리에 따른 무선 인터넷(Wi-Fi) 속도 및 지연시간 비교 분석,” 한국통신학회 종합학술발표회(하계), pp.974-975, 2011년 6월.

[3] 육정수, “Snort Wireless 기반의 무선 침입방지 시스템에 관한 연구”, 배재대학교 대학원 석사 학위논문, 2014년 6월.