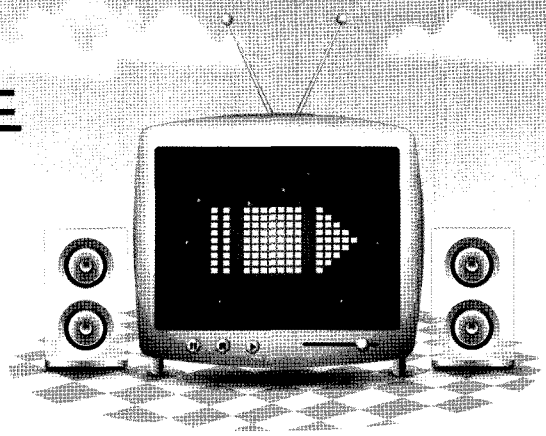
국내 Wi-Fi 보안 현황 및 안전한 무선랜 이용 가이드



백종현 | 한국인터넷진흥원 무선인터넷팀장

1. 머리말

최근 스마트폰 및 태블릿 PC 보급은 언제 어디서나 편리하게 인터넷을 할 수 있는 환경을 가져다줌으로써 우리 생활의 많은 부분을 바꾸어 놓았다. 이러한 무선 인터넷 환경에서 부각된 중요 기술 중 하나가 무선랜(Wireless LAN) 기술이다.

기존 국내 무선인터넷은 이동통신사의 고비용 폐쇄적인 3G 네트워크를 이용한 데이터 통신 위주로 이루어져 왔다. 특히 유선 인프라가 잘 갖추어진 국내에서는 내부 구조변경이 잦은 백화점, 일부 연구소 및 기업 환경 등에서 제한적으로 무선랜이 사용되어 왔다.

이러한 배경에서 스마트폰의 등장은 무선랜 확산을 가속화 시켰다. 스마트폰은 이동통신사의 네트워크와 무선랜을 모두 이용 가능하다. 상대적으로 저렴하고 빠른 통신 속도를 가진 무선랜을 선호함으로써 가정, 학교, 공중시설 등을 중심으로 무선랜이 널리 보급되는 동시에 다양한 무선랜 이용 환경이 만들어졌다.

무선랜은 다양한 장점과 편의성을 가지고 있어 이용이 급증하고 있지만, 전파를 통신매개로 이용하는 특징에 따라 보안을 고려하지 않고 이용할 경우 일반적인 유선랜(LAN)에 비해 더욱 취약하다. 특히, 공중 무선랜과 같이 일반 대중의 사용을 목적으로 개방된 환경의 경우 다양한 보안 사고를 유발할 수 있어 보안에 대한 고려가 필수적이다.

본 고에서는 국내 무선랜 이용환경 및 구축현황을 살펴보고 무선랜 환경별 보안위협을 분석한다. 또한 제시된 무선랜 환경별 보안위협에 따른 대응방안을 설명한다.

2. 무선랜 기술

무선랜이란 유선랜과 대비되는 표현으로 무선으로 네트워크를 이용할 수 있도록 하는 기술을 통칭하며 국제 표준화 기구인 IEEE에서 802 위원회의 하부 그룹인 802.11 그룹에서 표준화를 진행 중이다. 현재까지 제정된 무선랜 관련 주요 표준은 〈표 1〉과 같다.[1]

또한 국제표준인증단체인 Wi-Fi Alliance에서는 IEEE에서 제정한 무선랜 표준을 만족하는 장치에 표준 적합 인증마크를 부여하고 있다. 대부분의 무선랜 관련 장치에는 와이파이(Wi-Fi) 인증마크가 부착되는데 이러한 이유로 흔히 무선랜과 와이파이라는 표현은 혼

용되어 사용되고 있다.[2]

〈표 1〉 무선랜 기술표준 및 특징

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

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.

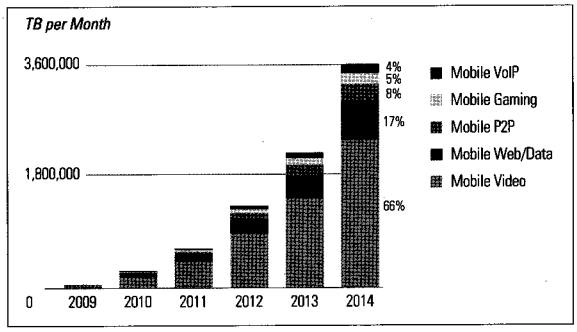
〈표 2〉 무선랜 보안기술

구분	WEP	WPA	WPA2
인증	PSK	PSK or 인증서버	PSK or 인증서버
암호화	RC4	RC4-TKIP	AES-CCMP

※TKIP: Temporal Key Integrity Protocol
CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

3. 무선랜 현황

스마트폰은 단순한 음성 통화기능 외에 인터넷전화, 모바일 게임, 모바일 웹, 모바일 비디오 등 데이터 통신을 이용하는 다양한 기능을 제공하고 있어 스마트폰 출시를 계기로 모바일 트래픽 사용량은 증가했다. 태블릿 PC, 와이파이 제공 피처폰(feature phone) 등 다양한 형태의 모바일 단말기가 출시되고 다양한 모바일 서비스가 활성화됨에 따라 향후에도 모바일 데이터 트래픽은 지속적으로 증가할 것으로 예상되고 있다.[3]



※출처: CISCO(2010.2)

[그림 1] 모바일 트래픽 전망

이동통신사에서는 이동통신 네트워크만으로는 급증하는 모바일 트래픽을 수용하기 어려워짐에 따라 분산처리를 위한 대체 망 확보가 시급하게 되었고 이에 따라 무선랜이 주목받게 되었다.

무선랜은 공공 주파수 대역을 사용하므로 전파 사용료 지불 및 송출 허가가 불필요하고 무선 AP의 가격이 저렴하여 단기간에 구축하기 적합하다. 또한 사용자 입장에서도 기존 이동통신 네트워크보다 빠른 속도와 저렴한 이용료로 이용할 수 있는 장점이 있다.

이러한 무선랜의 장점으로 2010년 상반기부터 경쟁적으로 이동통신사의 무선랜 구축이 이루어졌으며, 그 결과 국내에서는 2010년 11월 현재 약 7만 곳 이상의 와이파이존이 구축되어 운용되고 있다. 〈표 3〉에서는 국내 이동통신 사업자가 구축한 와이파이존 현황을 보여주고 있다.

한편 국내에서는 무선 공유기를 함께 제공하는 인터넷 전화 보급 확대와 저렴한 무선 공유기 판매로 일반 가정에서도 무선랜을 구축하는 사례가 증가하고 있다. 또한 은행, 호텔, 레스토랑, 공항 등 공공시설에서도 고객 편의제공을 위한 무선랜 접속시설을 확대하는 등

전국적으로 무선랜을 이용할 수 있는 환경이 조성되고 있다.

〈표 3〉 국내 이동통신 3사 와이파이존 구축 현황

[단위 : 곳]

이동통신사	2009년 말	2010년 7월	2010년 11월
KT	약 12,000	27,000	40,000
SKT	-	5,000	14,000
LG U+	-	-	16,000
계	약 12,000	32,000	70,000

※출처: 각 사업자 발표, 언론보도

〈표 4〉 국내 인터넷전화 보급현황

[단위 : 천 명]

구분	2007	2008	2009
KT	32	328	1,701
SK브로드밴드	47	121	1,333
LG 텔레콤	212	1,203	2,216
합계	291	1,943	7,103

※출처: 방송통신위원회/정보통신산업진흥원 재인용(2010.7)

4. 국내 무선랜 환경

국내 무선랜 이용환경은 구축 주체, 관리 주체, 이용 주체에 따라 크게 다섯 가지로 구분되며 세부 특징 및 보안 현황은 다음과 같다.[4]

4.1 상용 무선랜 환경

이동통신 사업자가 자사 고객 서비스용으로 구축·운영하는 무선랜 환경으로 사업자 이용 정책에 따라 개방형과 폐쇄형으로 나뉜다. 상용 무선랜 환경 중 개방형 환경은 자사 고객뿐만 아니라 타사 고객까지 이용을 허가하는 환경을 의미하며 자사 고객의 경우 USIM(Universal Subscriber Identity Module), MAC(Media Access Control), ID/Password 등을 통해 이용하고, 타사 고객의 경우 실명인증 등의 방법을 통해 이용하는 방식이다. 폐쇄형 환경은 자사 고객에 대해서만 접속을 허용한다.

특히, 최근 무선랜 구축이 마케팅의 방법으로 대두되면서 경기장, 해수욕장, G20 정상 회담과 같은 각종 행사 장소 등지에 한시적인 무료 와이파이존을 구축하기도 했다.

4.2 공중 무선랜 환경

고객들이 무료로 이용할 수 있도록 공공기관, 호텔, 카페 등에서 공중 시설에 구축한 무선랜 환경을 의미하며 이동통신사가 구축한 무선랜 환경이 주로 자사 가입자 중심인데 반해 공중 무선랜 환경의 이용자는 해당 사업자를 방문하는 모든 고객이 대상이다. 공중 무선랜 환경은 소규모 환경으로서 별도의 보안 관리자를 두고 있지 않아 상대적으로 보안이 취약한 편이다.

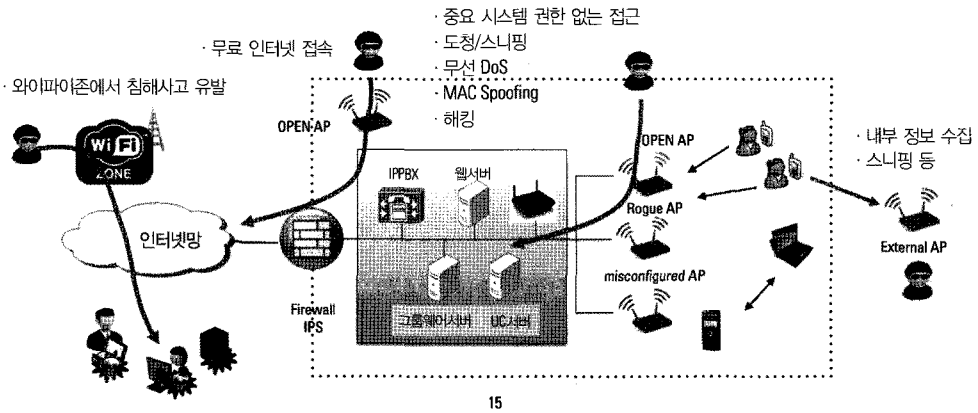
4.3 사설 무선랜 환경

일반인들이 전자상가 등지에서 구매한 무선공유기를 임의로 설치하여 운영하는 환경으로 자신 또는 주변인만 이용 가능하도록 구축한 환경이다. 무선공유기는 보안 기능은 탑재되어 있으나, 초기에 보안이 설정되어 있지 않고 이용자가 보안설정 지식 및 인식부족, 편의성을 이유로 보안을 설정하지 않고 이용하는 사례가 많다.

4.4 인터넷전화용 무선랜 환경

인터넷전화 설치 시에 제공되는 무선랜 환경으로서 인터넷전화용 무선공유기는 인터넷전화용과 데이터 통신용의 두 가지 무선랜을 동시에 제공한다. 인터넷전화용 무선랜의 경우 보안이 설정되어 있고 무선랜 정보가 숨겨져 있기에 비교적 안전하지만 데이터 통신용 무선랜의 경우 외부에 알려진 초기 패스워드 사용으로 무단접속, 정보유출 등 다양한 보안위협이 있다.

최근 이러한 문제를 개선하기 위해 인터넷전화 사업



[그림 2] 무선랜 보안위협

자들은 초기 패스워드를 기기마다 다르게 설정해 출시하고 있으나, 기존 보급된 인터넷전화용 무선랜의 경우 안전한 이용이 필요하다.

4.5 기업 무선랜 환경

기업이 내부 업무용으로 구축한 무선랜 환경을 의미하며 최근 스마트폰을 이용한 스마트 오피스, 스마트 워크 도입이 확산됨에 따라 점차 구축사례가 증가하고 있다. 기업 유선 네트워크로 접근할 경우 Firewall, IDS(Intrusion Detection System) 등 다양한 보안 시스템들로 내부망을 보호할 수 있으나 무선 네트워크의 경우 유선상의 보안 장치들을 우회 접근할 수 있어 별도의 보안 시스템 적용이 필수적이다.

일반적으로 기업 무선랜 환경에서는 무선 AP 자체의 보안 설정, 인증서버 구축을 통한 인증 및 접근제어, WIPS(Wireless Intrusion Prevention System) 등 다양한 보안 시스템을 적용하고 있다.

5. 무선랜 보안위협 및 대응방안

무선랜은 전파를 이용해 통신하므로 물리적인 접근 없이 무선랜 서비스를 이용할 수 있고 전파 수집 및 교란을 통한 다양한 보안위협을 야기할 수 있다. [그림 2]에서는 무선랜을 통한 보안위협을 보여주고 있다.[5]

본 장에서는 무선랜에서의 보안위협을 기술적인 측면과 함께 관리적, 물리적 측면으로 나누어 무선랜 보안위협과 대응방안을 설명한다.

5.1 기술적 보안 위협

무선랜의 기술적 보안위협은 전파수집, 불법접속, 중간자 공격(Man in the Middle Attack) 등을 통한 사용자 주요정보 유출과 전파 교란(Jamming), 다량의 패킷 전송을 이용한 서비스거부 공격이 있으며 WEP 등 취약한 보안설정을 해킹해 불법접속 및 내부 망으로 침투하는 등 다양한 공격유형이 있다.

무선랜의 기술적 보안위협은 WPA2 등 무선 AP에서 제공하는 보안을 설정함으로써 대부분 차단가능하다. 하지만 기업환경 등 중요정보를 취급하는 장소에서 무선랜 이용은 WIPS 등 전문 무선 보안 시스템 도입이 필수적이다.

5.2 관리적 보안 위협

무선랜에 강력한 보안기술을 적용하여도 적절한 관리가 이루어지지 않는다면 이를 쉽게 우회할 수 있다.

관리적 보안위협으로는 무선랜 장비 및 단말 관리 미흡, 사용자 보안의식 결여로 인한 침입허용, 전파관리 미흡에 따른 외부자의 내부 AP 접속 및 내부자의 외부 AP 접속 허용 등이 있다.

무선랜 관리적 보안위협의 대응 방안으로는 AP와 같은 접속장치 및 단말에 대한 관리방안을 수립 · 실시하고, 이용자들에 대한 주기적인 인식제고 및 교육, 내 · 외부 불법 접속에 대한 점검 등을 실시해야 한다.

5.3 물리적 보안 위협

유선인터넷 환경의 네트워크 장비들이 대부분 일반 사용자가 접근하기 어려운 곳에 설치 · 관리 되는 것에 비해, 무선 AP는 전파송출의 필요성 등으로 외부에 노출되어 설치되는 경우가 많다. 이러한 경우 무선 AP는 도난/파손, 전원차단, 랜선 분리 등의 위험이 있으며, 서비스에 장애 상태가 발생할 수 있다. 또한 무선단말기가 분실되어 저장된 무선랜 접속정보 및 보안설정 정보가 유출될 경우 비인가자의 무선랜 접속을 허용할 수 있다.

이와 같은 위협에 대비하기 위해서는 무선 AP가 외부에 노출되지 않도록 하고 설정정보를 주기적으로 변경하며 동시에 무선랜을 이용하는 단말 관리 및 분실 대비 방안을 강구해야 한다.

5.4 기타 보안 위협

최근 인터넷전화 보급 및 공중 무선랜 구축이 증가하게 되면서 새로운 보안위협이 등장하고 있다.

먼저 인터넷전화의 경우 초기 패스워드가 외부로 알려져 있으나 인터넷전화 사용자들이 보안지식 및 인식 부족으로 이를 변경하고 이용하지 않아 이를 통한 다양한 보안사고 발생 위협이 있다. 따라서 사업자 및 정부차원에서 무선랜의 보안위협을 충분히 인지시키고 이용자들이 스스로 또는 사업자들이 서비스 제공시 보안설정 및 암호 변경을 하도록 유도해야 한다.

공중 무선랜의 경우 누구나 이용할 수 있도록 구축되어져 있어 일반인뿐만 아니라 해커가 접속할 수도 있다. 이러한 경우 악성코드 유포 및 스팸발송의 근원지가 될 수 있으며 공중 무선랜에서 침해사고 발생 시 무선 AP까지만 추적이 가능하여 대응에 어려움을 야기할 수 있다. 따라서 공중 무선랜 구축 시에는 이용자 접속관리 시스템 등 침해사고 추적을 위한 장치가 필요하다.

6. 맺음말

2009년 하반기부터 시작된 스마트폰 열풍으로 무선랜 이용은 급격히 증가했다. 무선랜 기술이 갑자기 등장한 것은 아니지만 이동통신사업자의 적극적 무선랜 인프라 활용, 유무선 융합 서비스 출시, 다양한 형태의 사설 무선 AP 보급 등으로 다양한 환경에서 무선랜을 사용하게 됨으로써 무선랜은 점차 필수적인 서비스가 되고 있다.

무선랜의 전송 특성상 보안의 고려는 필수적이지만 무선랜 이용환경의 다양화로 인해 일관된 보안정책 적용에 어려움이 있기에 다방면으로 보안강화를 위한 노력을 추진해야 한다.

정부에서는 사설 무선랜에 보안을 강화할 수 있도록 보안설정 지식을 제공하고 무선랜 보안 홍보를 통해 대국민 인식제고를 추진하고 있다. 이동통신 사업자들은 정부와 협조를 통해 상용 무선랜에서 보안사고 대응체계를 수립하는 동시에 인터넷 전화 등 가정용 무선랜 상품에 대한 보안 대책을 추진해야 한다. 이 외, 기업의 전산운영자 및 보안담당자들은 자사 운영 무선랜에 대한 보안관리 체계를 수립하고 주기적인 점검을 통해 보안사고 발생을 최소화해야 한다.

안전한 무선랜 이용을 위해서는 무엇보다 개개인이

무선랜 보안위협을 이해하고 안전한 무선랜 이용의 필요성과 방법을 지키는 것이 필요하다.

[참고문헌]

[1] http://standards.ieee.org/getieee802/802.11.html

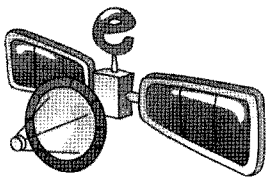
[2] http://www.wi-fi.org/

[3] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2009–2014(CISCO, 2010.2.9)

[4] 백종현, 'Wireless LAN Status and Security Issues in Korea' CJK SWIS 2010, 2010.11

[5] 한국인터넷진흥원 '무선랜 보안 안내서' 2008 TTA

정보통신용어해설



스마트 페이먼트

Smart Payment [통신서비스]

스마트폰 등으로 결제하는 방식.
기존의 카드 결제, 멤버십, 쿠폰, 포인트 따위를 스마트폰으로 처리하는 서비스를 말한다. 스마트폰만 들고 다니면 자동으로 결제가 진행되기 때문에 굳이 신용카드, 교통카드 들을 가지고 있을 필요가 없다. 다만, 스마트 페이먼트를 지원하는 스마트폰이 필요하다.