무선랜 이용 환경별 보안위협 및 대응방안

박순태*, 원용근*, 백종현*
*한국인터넷진흥원
e-mail:{cptpark | ygwon | jhbaek}@kisa.or.kr

A Study on Security Threats and Countermeasure for WLAN Environment

Soon-Tai Park*, Yong-Geun Won*, Jong-Hyun Baek*
*Korea Internet & Security Agency

요 약

최근, 스마트폰 등 무선랜 이용가능 단말기의 출시와 저렴한 무선 AP(Access Point) 보급 확대로 무선랜 이용이 급속히 확대되고 있다. 그동안 국내 무선인터넷 환경은 이동통신사가 구축한 고비용 폐쇄적 3G 네트워크의 데이터 통신 위주로 이루어졌으며, 무선랜 이용은 일부 기업환경 및 호텔/식당 등의 고객용 무선랜, 개인용 무선랜 등으로 한정되어 사용되었다. 하지만 '10년 스마트폰의 폭발적인 확산으로 무선랜을 통해 빠르고 저렴하게 무선 인터넷을 사용할 수 있게 됨에 따라 가정, 공공시설 등에서 무선랜 구축/활용이 매우 증가하고 있다. 논문은 무선랜에 대한 물리적, 기술적, 관리적 보안위협을 살펴보고 구축, 관리, 이용 주체별 대응방안을 제시한다.

1. 서론

최근, 스마트폰 등 무선랜 이용가능 단말기의 출시와 저렴한 무선 AP(Access Point) 보급 확대로 무선랜 이용이 급속히 확대되고 있다.

그동안 국내 무선인터넷 환경은 이동통신사가 구축한 고비용 폐쇄적 3G 네트워크의 데이터 통신 위주로 이루어졌으며, 무선랜 이용은 일부 기업환경 및 호텔/식당 등의 고객용 무선랜, 개인용 무선랜 등으로 한정되어 사용되었다. 하지만 '10년 스마트폰의 폭발적인 확산에 따라 무선랜을 통해 빠르고 저렴하게 무선 인터넷을 사용할 수 있게 됨에 따라 가정, 공공시설 등에서 무선랜 구축/활용이 매우 증가하고 있다.

가정에서는 저렴한 무선랜 접속장치(무선 AP)가 확대되고 무선 AP를 함께 제공하는 인터넷전화가 확산되면서 가정에서 무선 AP를 흔히 볼 수 있게 되었다. 2010년 상반기 사설 무선 AP와 인터넷전화용 AP 등 국내에는 약 500여만 대가 보급된 것으로 확인되고 있다.

사용자 입장에서도 무선랜 이용은 요금에 구애받지 않고 3G 데이터통신에 비해 5~10 가량 빠르기 때문에 더욱 선호되고 있는 실정이다.[1]

한편 이통동신 사업자 측면에서는 스마트폰을 통한 무선인터넷 이용이 급증함에 따라 모바일 트래픽이 급증하게 되어 기존 3G 네트워크에서 수용한계에 다다름에 따라 우회 망으로 무선랜을 활용하고 있으며, 동시에 빠르고 편리한 무선랜 인프라가 곧 고객유치를 위한 중요한 요소로 인식되어 다양한 장소에서 무선랜을 구축하고 있다.[2]

무선랜은 다양한 장점과 편의성을 가진 반면, 전파를 통신매개로 이용하는 특성에 따라 보안을 고려하지 않고 이용할 경우 일반 유선랜에 비해 더 취약할 수 있으며, 공중 무선랜과 같이 관리주체가 불명확 한 경우 다양한 보안사고를 유발할 수 있어 보안에 대한 고려가 필수적이다.

본 논문에서는 국내 무선랜 구축현황을 통해 구축/관리 주체로 구분하여 무선랜 환경을 분류하고 각 무선랜 환경별 보안위협을 분석한다. 또한 무선랜 환경별 보안 대응방안을 기술하여 안전한 무선랜 이용환경 모델을 제시한다.

2. 무선랜 기술 및 운용환경

무선랜(Wireless LAN)이란 선 연결 없이 전파를 이용하여 인터넷 서비스를 제공하는 기술을 의미하며, 일반적으로 와이파이(Wi-Fi)라고 불린다. 무선랜 관련 표준화는 IEEE에서 802 위원회의 하부 그룹인 802.11 그룹에서 다루고 있으며 현재까지 제정된 무선랜 관련 주요 표준은 <표 1>과 같다.[3]

<표 1> 무선랜 기술표준 및 특징

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

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.[4][5]

<표 2> 무선랜 보안기술

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

PSK는 Pre-Shared Key의 약자로서, 비밀번호를 입력하는 인증방법을 의미하며, TKIP와 CCMP는 암호키 동적 변경 및 암호알고리즘 강화 기법이다.

한편, 국내 무선랜 이용환경은 구축 및 관리 주체, 이용 대상의 특성에 따라 다음과 같이 분류할 수 있다. 구축 주체는 사업자(Business), 개인(Private), 관리 주체도 사업자(Business), 개인(Private)로 구분할 수 있으며, 이용 주체는 특정인(Known), 불특정 다수(Unknown)로 구분할 수 있다.

<표 3> 무선랜 이용 환경 구분

구축/관리 / 이용자	사업자 구축(Business)		개인 구축 (Private)
	사업자 관리 (Business)	개인 관리 (Private)	개인 관리 (Private)
특정인 (Known)	①	②	③
불특정 다수 (Unknown)	④	⑤	⑥

① B-B-K : 사업자구축-사업자관리-특정인이용 형태로 자사 가입자가 유·무형의 대가를 지불하고 이용하는 무선랜이다. 사업자가 초고속인터넷과 함께 결합상품의 하나로 무선랜을 제공하는 경우가 해당된다.

② B-P-K : 사업자구축-개인관리-특정인이용 형태로 가정에서 서비스 신청 시에 통신사업자가 설치한 무선랜으로 해당 서비스로는 가정용 무선인터넷 서비스, 인터넷전화서비스에서 제공하는 무선랜 등이 있다.

③ P-P-K : 개인구축-개인관리-특정인이용 형태로 개인이 무선 AP기기를 직접 구매 및 설치한 무선랜 환경이다. 주로 가정에서 사용되며 기업의 업무용 무선랜도 동일한 유형으로 포함한다.

④ B-B-U : 사업자구축-사업자관리-불특정다수이용 형태로 누구나 사용할 수 있도록 통신사업자가 공중시설에 설치한 무선랜이다. 최근 이동통신사가 경쟁적으로 구축하고 있는 와이파이존에 해당한다.

⑤ B-P-U : 사업자구축-개인관리-불특정다수이용 형태로 인터넷전화서비스에 제공된 무선 AP를 개방하여 활용하는 경우에 해당한다.

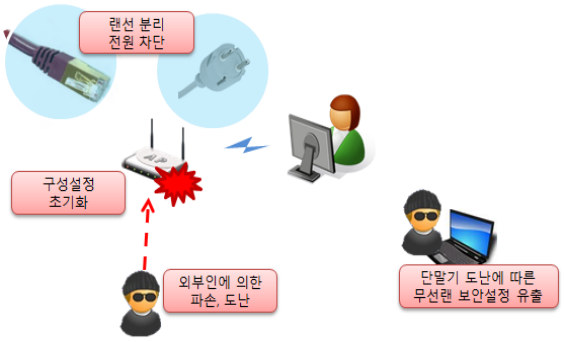
⑥ P-P-U : 개인구축-개인관리-불특정다수이용 형태로 카페, 식당 등 SOHO와 같이 고객 편의제공을 위해 구축한 무선랜이다.

3. 무선랜 유형별 보안위협

무선랜은 전파를 이용하여 통신하므로, 물리적인 접근뿐만 아니라 접근 없이도 무선랜 서비스를 이용할 수 있어, 다양한 보안위협에 노출된다. 무선랜 공격 유형을 장비 훼손, 시스템 및 네트워크 해킹, 공격대상 정보수집으로 구분한 사례는 있으나 본 논문에서는 물리적, 관리적, 기술적, 기타 보안위협으로 구분 한다.[6]

3.1. 물리적 보안 위협

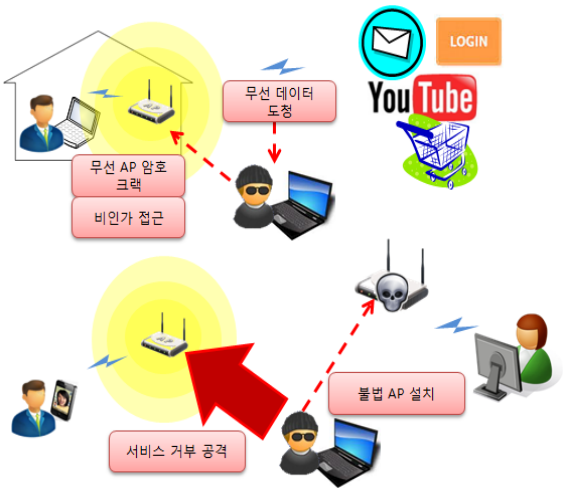
무선랜의 물리적 보안위협은 (그림 1)과 같다. 무선 AP의 도난/파손, 전원차단 등이 발생할 경우 서비스에 장애 상태가 발생할 수 있다. 또한, 무선단말기가 분실되어 저장된 무선랜 접속정보 및 보안설정이 유출될 수 있다.



(그림 1) 무선랜의 물리적 보안위협

3.2. 기술적 보안 위협

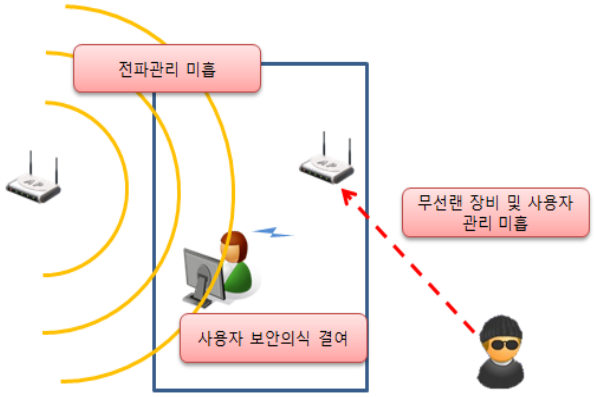
무선랜의 기술적 보안위협은 (그림 2)와 같다. 전파수집, Man in the Middle Attack 등을 통해 사용자의 주요 정보나 접속행위가 노출될 수 있으며 전파 교란, 다량의 패킷 전송으로 서비스거부 공격을 할 수 있다. 또한 WEP 등 취약한 보안설정을 한 경우 패스워드가 해독될 수 있다. 이 경우 노출된 패스워드 및 인증의 취약점을 이용하여 비인가 사용자가 접근하게 될 수 있다.



(그림 2) 무선랜의 기술적 보안위협

3.2. 관리적 보안 위협

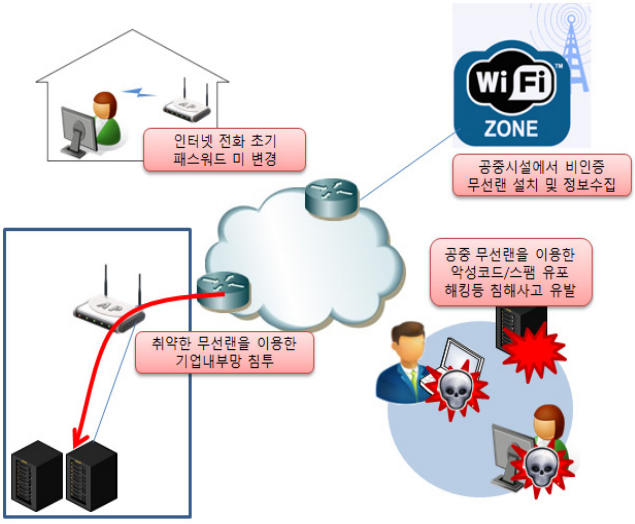
무선랜의 관리적 보안위협은 (그림 3)과 같다. 무선 AP가 비인가자에게 무단으로 사용될 경우 외부로부터 침입의 통로를 제공하게 된다. 무선 AP에 대한 관리·접속 비밀번호는 별도로 관리하고 주기적으로 변경되어야 한다.



(그림 3) 무선랜의 관리적 보안위협

3.4. 기타 보안 위협

기타 무선랜 보안위협은 (그림 4)와 같다. 최근 구축되고 있는 공중 무선랜의 경우 누구나 접속 가능하므로 해커가 접속하여 침해사고를 발생할 수 있다. 또한 인터넷전화 서비스에서 제공하는 가정용 무선랜의 경우 SSID 인증키로 공개된 비밀번호로 설정되어 있으면 외부인이 무단으로 사용 하거나 개인정보를 유출할 수 있다.



(그림 4) 기타 무선랜 기반 보안위협

4. 안전한 무선랜 이용 방안

3장에서 구분한 무선랜 보안위협을 정리하면 <표 4>와 같다. 이러한 보안위협은 <표 5>와 같이 위협에 따른 대응 방안이 필요하다. <표5>는 제안하는 방안이 도출된 위협에 대응함을 보여준다.

<표 4> 무선랜 유형별 보안위협

구 분	세부 위협 내용	
물리적 보안 위협	TP01	무선 장치에 대한 물리적 보안위협
	TP02	무선 단말기에 대한 물리적 보안위협
기술적 보안 위협	TT01	무선랜 이용자에 대한 도청
	TT02	무선 AP에 대한 서비스 거부
	TT03	불법 AP(Rogue AP)설치
	TT04	무선AP에 설정된 암호 크랙
	TT05	무선랜에 대한 비인가 접근
관리적 보안 위협	TM01	무선랜 장비 관리 미흡
	TM02	무선랜 사용자의 보안의식 결여
	TM03	전파관리 미흡
기타 보안 위협	TE01	공중 무선랜을 이용한 악성코드/스팸 유포
	TE02	기업용 무선랜으로 기업 내부 네트워크 침투
	TE03	초기 보안설정 유지에 따른 무단접속 허용

<표 5> 무선랜 정보보호 대응 방안

구분		정보보호 대응 방안	
정책 및 관리	현황 및 장비	DME01	무선랜 사용자 현황 파악
		DME02	무선랜 장비 현황 파악
		DME03	무선랜 장비에 대한 물리적 보호
		DME04	무선랜 장비 관리 프로그램 보호
		DME05	무선랜 사용에 관한 보안 정책 정의
	네트워크	DMN01	SSID 설정
		DMN02	채널 설정
		DMN03	전파 출력 세기
보안기술(솔루션) 도입		DTS01	무선랜 데이터 암호화
		DTS02	사용자 인증
		DTS03	키 관리
		DTS04	보안 솔루션 적용 및 무선랜 운용 상황 감시
정보보호 인식제고		DSA01	주기적 보안 점검
		DSA02	보안 교육
		DSA03	시스템 보안 기능의 설정 및 주기적 패치

<표 6> 무선랜 보안위협과 대응방안 매핑표

구분	DME01	DME02	DME03	DME04	DME05	DMN01	DMN02	DMN03	DTS01	DTS02	DTS03	DTS04	DSA01	DSA02	DSA03
TP01			○		○								○	○	
TP02			○		○								○	○	
TT01					○				○	○			○	○	
TT02					○							○	○	○	
TT03		○			○					○		○	○	○	
TT04					○				○				○	○	
TT05	○				○	○			○	○	○	○	○	○	
TM01			○	○	○						○		○	○	○
TM02					○								○	○	
TM03					○		○	○				○	○	○	
TE01					○							○	○	○	
TE02					○					○			○	○	
TE03					○						○		○	○	○

무선랜 정보보호 대응방안은 물리적, 기술적, 관리적, 기타 위협에 대하여 보안정책 및 관리, 보안기술 도입 및 적용, 정보보호 인식제고로 분류할 수 있다. 세부 방법으로는 무선랜 서비스 제공자의 입장에서 무선랜 보안 구축 지침 및 운영 가이드, 내부 관리 지침 등 보안정책에 입각하여 구축 및 운영이 필요하다.[7][8] 또한 인증서버, 전용 보안 솔루션 등 무선랜 보안기술을 도입하여 보안성을 강화할 수 있다. 이외 무선랜 서비스 이용자의 입장에서는 이용자 개개인이 보안인식을 가지고 무선랜을 안전하게 이용하는 것이 중요하다.[9] 무선랜 정보보호 대응방안은 2장에서 분류한 이용 환경별로 적용할 수 있다. 이를 표로 나타내면 <표 7>과 같다.

<표 7> 무선랜 이용 환경별 정보보호 추진 방향

무선랜 이용 환경			서비스 측면	보안정책 및 관리	보안기술 도입	정보보호 인식제고
구축	관리	이용				
사업자 (B)	사업자 (B)	특정인 (K)	제공자	○	◎	△
			이용자	△	△	○
		불특정 (U)	제공자	◎	◎	○
			이용자	△	△	◎
	개인 (P)	특정인 (K)	제공자	△	○	◎
			이용자	△	△	◎
		불특정 (U)	제공자	○	○	◎
			이용자	△	△	◎
개인 (P)	개인 (P)	특정 (K)	제공자	△(◎)	△(◎)	◎
			이용자	△	△	◎
		불특정 (U)	제공자	◎	○	◎
			이용자	○	○	◎

범례 : ◎ 매우 필요, ○ 필요, △ 선택적 필요

※ ( )는 기업 무선랜 환경

B-B-K 환경은 통신사업자가 구축하는 무선랜 환경으로서, 보안사고 발생 시 사업자의 책임소재가 크므로 보안 솔루션 등의 도입이 매우 중요하다. B-B-U 환경의 경우도 통신사업자가 운영하지만 누구나 자유롭게 접속할 수 있는 특성상 보안 솔루션과 함께 보안정책 수립이 필요하며, 이용자 또한 서비스 이용에 주의할 수 있도록 인식 제고가 필요하다. B-P-K 및 P-P-K 환경의 경우 주로 가정에서 설치, 운영되는 특성상 보안정책 및 기술 도입이 어려운 측면이 있으며 이용자의 인식제고를 통해 무선 AP 자체의 보안기능을 활용하여 안전하게 이용하는 것이 필요하다. 그러나 기업용 무선랜의 경우에는 보안 솔루션 및 보안정책의 도입이 필수적이다. B-P-U 및 P-P-U 환경의 경우 대 고객 서비스 또는 무선랜 활성화 측면에서 무선랜이 제공되므로 누구나 접속 가능하여 보안 솔루션 도입이 어려워 보안이 취약한 환경이다. 이를 위해서는 보안정책 제공 및 인식제고가 필요하다.

5. 결론

지금까지 무선랜 기술 및 운용 환경, 유형별 보안 위협 및 안전한 무선랜 이용 방안을 살펴보았다. 안전한 무선랜 이용을 위해서는 다양한 무선랜 환경별로 구축 단계에서 보안을 설정하여 구축하여야 한다. 운영 단계에서는 관리자가 보안의 중요성을 인식하여 보안 정책 수립 및 기술 도입, 보안설정을 하여야 한다. 마지막으로 이용 단계에서는 이용자의 보안 인식을 제고하여 보안 사고를 예방하고, 안전하게 무선랜 서비스를 이용할 수 있도록 해야 한다.

참고문헌

[1] 이상준, “무선랜 이용 확산과 보안 이슈 및 대응”, 제15회 정보보호 심포지엄. 2010.6

[2] 김재섭, “통신 3사, 무선망 확대에 승부 걸었다”, 한겨레 신문, 2010.7

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

[4] Johnny Cache, Vincent Liu, "Hacking Exposed Wireless", 2007

[5] Gunther Lackner, "Wireless-Network Security: Basics Knowledge", 2008

[6] 정보통신단체표준 TTAS.KO-12.0031, "안전한 무선랜 사용을 위한 가이드", 한국정보통신기술협회, 2005.12

[7] “정보통신보안업무규정”, 행정안전부, 2009.6

[8] “무선랜 보안 가이드”, 방송통신위원회, 2010.1

[9] http://www.118.or.kr