금보원 2010-12

금융부문 무선랜 보안 가이드

2010. 12

금융보안연구원

본 가이드의 내용 중 오류가 발견되었거나, 내용에 대한 의견이 있을 경우 금융보안연구원 신기술분석센터(newtech@fsa.or.kr)로 해당 내용을 보내주시기 바랍니다.

머 리 말

현재 우리나라 은행의 전자금융거래 이용자 수는 약 6,390만 명(중복가입 포함, ′10. 09 末 기준)을 넘어섰으며, 스마트폰 뱅킹 등록고객 수도 약 137만 명(한국은행, ′10. 09 末 기준)이 되는 등 금융회사의 전자금융 거래 이용자 수는 매년 빠른 속도로 증가하고 있습니다. 정보기술의 발달에 힘입어 모바일을 이용해 이동하면서 주식거래를 하는가 하면 안방에서 TV를 활용해 은행거래 서비스를 이용하는 등 획기적인 전자금융 서비스가 속속 개발되고 있으며, 앞으로도 신규 전자금융 서비스는 그 편리함으로 인하여 이용이 지속적으로 증가할 것으로 예상됩니다.

최근 스마트폰의 활용도가 높아지면서 이에 따라 무선랜의 구축이 늘어나고 금융기관에서도 무선랜을 통한 업무의 활용도를 높임에 따라 무선랜의 안전성 및 신뢰성에 대한 중요도가 증대되고 있습니다. 또한 사용의 편의성으로 인해 쉽게 접속하고 사용할 수 있게 설치된 무선랜을 통해 유출되는 개인정보 및 중요한 데이터들에 대한 안전성을 확보하기 위한 안전한 무선랜의 구축이 필요한 실정입니다.

이에 금융보안연구원은『금융부문 무선랜 보안 가이드』를 개발하게 되었습니다. 이 가이드가 안전한 무선랜의 구축과 운영 그리고 안전한 전자금융 서비스 제공에 많은 도움이 되기를 바라며 가이드 작성에 직접 참여해 주신 전문가 여러분과 우리원 연구원들에게 깊은 감사를 드립니다.

2010년 12월
금융보안연구원
원장 곽 창 규

차례

금융부문 무선랜 보안 가이드

그림

금융부문 무선랜 보안 가이드

표

금융부문 무선랜 보안 가이드

제1장 개 요

제 1 절 배 경

2010년 스마트폰 사용자가 500만명을 돌파하였고, 대형 통신사에서 약 5만개의 와이파이존 구축이 진행 되고 있다. 여기에 통계되지 않는 인터넷전화 및 개인의 무선랜 사용을 더하면 그 수요는 늘어날 것이다. 무선 네트워크는 빠른 시간에 구축이 가능하며 이동성이 보장되는 장점과 비용효과적인 통신 솔루션으로 각광 받고 있다. 또한 장소에 상관없이 자유롭게 네트워크에 접속한다는 유비쿼터스 기술의 초석이 된다는 점으로 제조, 유통, 운송 및 금융 분야까지 무선 네트워크는 그 사용 영역이 확대되고 있다. 그러나 전파를 사용하여 데이터를 전송하는 무선랜은 가청 범위내에 존재하는 무선랜 전파를 무선랜카드와 데이터 수집 S/W를 통해 누구라도 쉽게 접근 할 수 있다는 점에서 유선랜 보다 보안적으로 취약한 점이 존재한다. 이러한 문제점을 해결하기 위해 다양한 보안 관련 기술이 개발 적용되고 있으나 안전하지 않게 구축된 무선랜으로 인해 이미 구축된 유선랜 보안장치들을 우회하여 내부의 기밀정보가 유출될 수 있는 가능성이 존재한다.

제 2 절 목 적

본 가이드를 통해 무선랜의 현황 및 발생 가능한 주요 취약점 및 위협을 분석하고 이를 해결하기 위한 관련 기술을 살펴본다. 또한 금융회사 및 관련업체에서 무선랜을 구축할 때 고려해야 할 주요 보안 고려사항에 대해서도 기술하였다.

제 3 절 범 위

본 가이드는 무선랜의 역사와 표준, 알려진 무선랜의 주요 취약점 및 위협을 기술하고 이를 해결하기 위한 관련 기술의 설정 및 대응책의 소개와 주요 보안 고려사항까지 그 범위에 속한다.

제2장

무선랜 서비스 현황

제 1 절 무선랜 기술표준 및 현황

1. 무선랜 기술표준

가. 무선랜 표준의 역사

무선랜의 역사는 1987년의 FCC[1]의 면허가 필요 없는 무선 주파수 대역 규정에서부터 시작되었다. 1990년 FCC가 인가한 19GHz의 주파수 대역을 사용하여 15Mbps까지 고속 전송이 가능한 제품을 Altair란 이름으로 1991년 발표하였다. 1997년 독자적으로 개발되던 무선랜 기술들을 한데 통합하여 IEEE[2]에서 802.11로 산업 표준화 시켰으며 1999년 9월 IEEE 802.11b 고속 무선 LAN 규격이 표준화되면서, 무선 LAN 시장은 급격한 성장을 맞이하게 된다. 이후 무선랜 표준은 꾸준한 보완작업이 이루어지며 802.11a, 802.11g를 거쳐 현재는 802.11n까지 표준으로 제정되었다.

1) FCC(Federal Communications Commission) : 미국 연방통신위원회
2) IEEE (Institute of Electrical and Electronics Engineers) : 국제 전기전자 기술자협회 무선랜 관련 표준 개발 기구

표 1 무선랜 표준 제정내용

무선랜표준	제정시기	주파수대역	데이터속도(최대)
802.11	1997	2.4GHz	2 Mbps
802.11a	1999	5GHz	54 Mbps
802.11b	1999	2.4GHz	11 Mbps
802.11g	2003	2.4GHz	54 Mbps
802.11n	2009	2.4GHz~5GHz	600 Mbps
802.11i	2004	-	-
802.11x	2004	-	-

나. 무선랜 표준의 주요 내용

그림 1 무선랜 표준 제정 연도

○ 802.11b는 2.4GHz 주파수 대역을 사용하며, 최대 11Mbps의 전송속도를 지원하며 38~140M의 접속반경을 제공한다.

○ 802.11a는 802.11과 802.11b와는 달리 5GHz의 주파수 대역을 사용하며, 최대 54Mbps의 전송속도를 지원하며 35~120m의 접속반경을 제공한다.

○ 802.11g는 802.11b와 같은 2GHz의 주파수 대역을 사용하지만, 전송방법을 OFDM[3]으로 수정을 통해 속도는 802.11a와 같은 최대 54Mbps를 지원한다. 802.11b와 호환을 이루면서도 속도의 향상을 가져와 현재 가장 널리 쓰이고 있는 표준이다.

○ 802.11n은 가장 최신 규격으로 2.4GHz와 5GHz 주파수 대역을 모두 지원하며 최대 600Mbps의 전송속도를 지원하며 70~250m의 접속반경을 제공한다.

○ 이 이외에 보안프로토콜을 개선한 802.11i와 유선포트 인증을 표준으로 EAP[4]를 정의한 802.1x 표준도 존재한다.

3) OFDM (Orthogonal Frequency Division Multiplexing; 직교 주파수 분할 다중) : 고속 양방향 무선 데이터 전송을 위한 효율적인 기술로 하나의 데이터를 다수로 분할하고 다중 전송하는 방식

4) EAP(Extensible Authentication Protocol) : 특정 인증메커니즘과 무관하게 인증 메시지를 교환하기 위한 프로토콜

표 2 무선랜 표준 보안 규격 내용

표준규격	표준 규격의 주요 내용
IEEE 802.11a	5GHz 주파수 대역에서 OFDM 변조 방식으로 최대 54Mbps의 물리계층 전송속도를 지원
IEEE 802.11b	2.4GHz 주파수 대역에서 CCK[5]/PBCC[6] 변조 방식으로 최대 11Mbps의 물리계층 전송속도를 지원
IEEE 802.11g	2.4GHz 주파수 대역에서 OFDM 변조 방식으로 최대 54Mbps의 물리계층 전송속도를 지원
IEEE 802.11n	물리계층에서 최대 600Mbps의 전송속도를 지원
IEEE 802.11i	802.1x, TKIP, AES 등을 도입하여 무선랜 인증/암호화 프로토콜의 보안 약점을 개선하기 위한 MAC[7]기능 강화
IEEE 802.1x	Port Based Network Access 표준안. 유선 포트의 인증을 위한 표준으로 EAP(Extensible Auth. Protocol)을 정의

범례 : 물리계층 프로토콜, 보안 프로토콜

5) CCK 방식 : 전송하고자 하는 비트를 미리 약속된 8비트 심볼로 바꾸어 전송하는 방식이다
6) PBCC 방식 : TI가 제창한 부호화 방식으로 CCK와 비교해 부호화 이득이 높은 방식
7) MAC(Media Access Control) 각각의 네트워크 장비에 유일하게 부여된 식별번호

2. 무선랜 서비스 현황

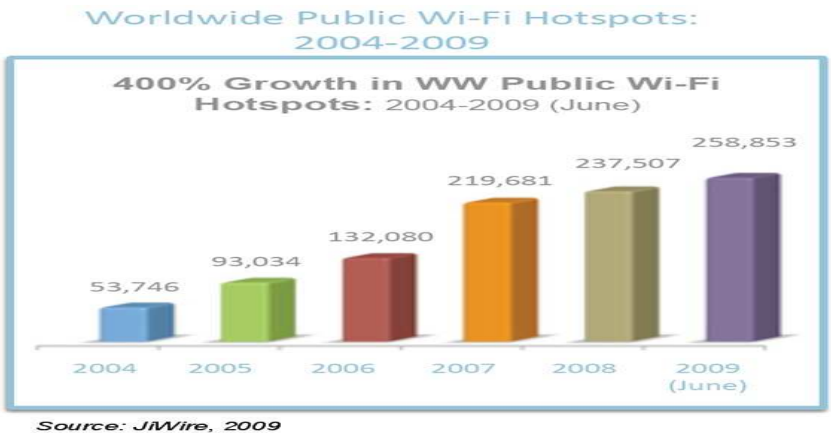


그림 2 세계 Hotspots zone 리포트[출처: JiWire 2009 보고서]

JiWire보고서에 따르면 전 세계의 Hotspots zone은 2009년 6월까지 2004년에 비해 약 400%가량 증가하였다.

Top 10 Countries for Public Wi-Fi: June 2009

Rank	Country	June 2009 # of Hotspots
1	United States	67,420
2	China	28,678
3	United Kingdom	27,459
4	France	25,619
5	Russian Fed.	14,499
6	Germany	14,435
7	South Korea	12,814
8	Japan	11,612
9	Sweden	6,664
10	Taiwan	5,386

Source: JiWire, 2009

그림 3 무선랜 분포 Top 10[출처: JiWire 2009 보고서]

"Mobile Audience Insights Report"에서 한국은 7번째로 Hotspots zone이 많이 존재하는 지역으로 조사되었다.

KT는 2010년 9월까지 와이파이존을 2만7000개 까지 늘리고, SK텔레콤도 신규로 1만개의 와이파이존 구축 계획을 밝혔으며 LG U+도 1만 1000개의 와이파이존을 구축할 예정이며 올해까지 약 5000개를 구축할 것으로 보인다.
이대로라면 무선인터넷을 사용할 수 있는 와이파이존은 통신 3사를 합쳐 2010년말에는 약 4만2000개 이상이 될 것이다.

무선랜 기반 인터넷전화가 확산되고 무선공유기 보급이 증대되고 있으며 정부와 지자체의 무선인프라가 확대되는 등 무선인터넷 활성화 정책이 본격적으로 추진되고 있다.

최근에는 스마트폰의 보급화로 인해 기업뿐 아니라 가정에서도 무선랜의 도입이 늘고 있으며 더불어 3G망과 무선의 기술을 연계하여 집 안에서는 인터넷 전화로, 외출 시에는 휴대폰으로 사용할 수 있는 FMC[8]의 도입이 고려되고 있다.

기업의 FMC이용과 인터넷 전화의 보급화로 인해 무선랜의 사용이 더 늘어날 것으로 보인다.

8) FMC(Fixed Mobile Convergence) : WLAN/CDMA dual mode 단말기에 기반하여, 기업 내에서는 무선 인터넷에 접속해 VoIP/데이터서비스를, 기업 외부에서는 이동통신망을 이용한 휴대폰으로 사용할 수 있도록 하는 유무선 통합 시스템

3. 세계 무선랜 보안 관련 주요 국가 제도

○ 해외의 무선랜 제공자에 대한 법규

표 3 해외의 무선랜 보안 법규 및 내용

국가	법규 및 내용
영국	디지털 경제법 일정 규모 이상의 ISP에 대해 무선랜 공급을 차단할 의무를 부여
미국 캘리포니아주	사업 및 직업법 무선 AP 상품의 생산자에게 무선랜 보안을 위하여 일정 의무 부과
미국 뉴욕주	공공인터넷보호법 최소한의 보안조치를 의무화 무선인터넷서비스를 제공하는 자는 이용자의 보안조치를 위한 안내 표지문 부착을 의무화
인도	Compliance Requirements 요구 와이파이 서비스를 제공하는 ISP에게 AP를 안전하게 하도록 할 의무 부여 사용자 등록제 및 로그인 시스템을 마련하도록 강제
나이지리아	Nigerian Communications Act 2003(통신법) 모든 통신기기들은 허가를 받아야 함 상업적 와이파이존에 대해 등록의무 부여 데이터보안 및 개인정보 보안을 위해 적정한 조치와 최소한 WEP/WPA 기준 충족을 의무화

❍ 국내의 무선랜 제공자에 대한 법규

표 4 국내의 무선랜과 관련된 법규 및 의무 주체

현행법	의무 주체
정보통신법	무선 AP 제공 사업자
법적 근거 없음	사설 무선 AP 사용자(개인, 기업)
전자정부법	공공무선랜을 운영하는 지방자치단체 및 공공기관
전파법	무선 AP를 수입 제조하여 판매하는 자
정보통신망법	호텔 등 고객대상 무선랜 서비스 제공자

제 2 절 무선랜 구성요소

1. 무선 네트워크 물리적 구성요소

그림 4 인증서버를 통한 무선랜 통신

가. 무선 AP

○ 무선 AP는 유선랜의 마지막에 위치하여 무선랜과 유선랜의 연결을 중계해주는 지점이다. AP는 무선랜 보안에 가장 큰 비중을 차지하는 중요한 장비로 AP가 지원하는 표준에 따라 무선랜의 인증방식과 전송 데이터 암호화 방식을 설정할 수 있다.

나. 무선 단말 및 무선랜카드

○ 사용자가 무선랜의 접속에 이용하는 장비를 말하며 그 종류는 무선랜에 접속할 수 있도록 전파를 송·수신 하는 기능을 가진 모든 종류의

무선장치를 말하고 특정한 무선랜을 접속하여 사용하기 위해서는 SSID, 인증 및 암호화 설정이 동일하여야 한다.

다. 인증서버

○ 무선랜 사용자의 인증을 위한 장비로 인증키를 관리하고 비인가 사용자의 접속을 제한하는 역할을 한다.

2. 무선 네트워크 기술적 구성요소

가. SSID

○ SSID는 무선랜을 통해 전송되는 패킷들의 각 헤더에 덧붙여지는 32 바이트 길이의 고유 식별자로서, 무선 장치들이 무선 네트워크에 접속할 때 네트워크 식별자처럼 사용된다. SSID는 하나의 무선랜을 다른 무선랜으로부터 구분해 주므로, 특정 무선랜에 접속하려는 모든 AP나 무선 장치들은 반드시 동일한 SSID를 사용해야만 한다.

나. 인증 및 암호화

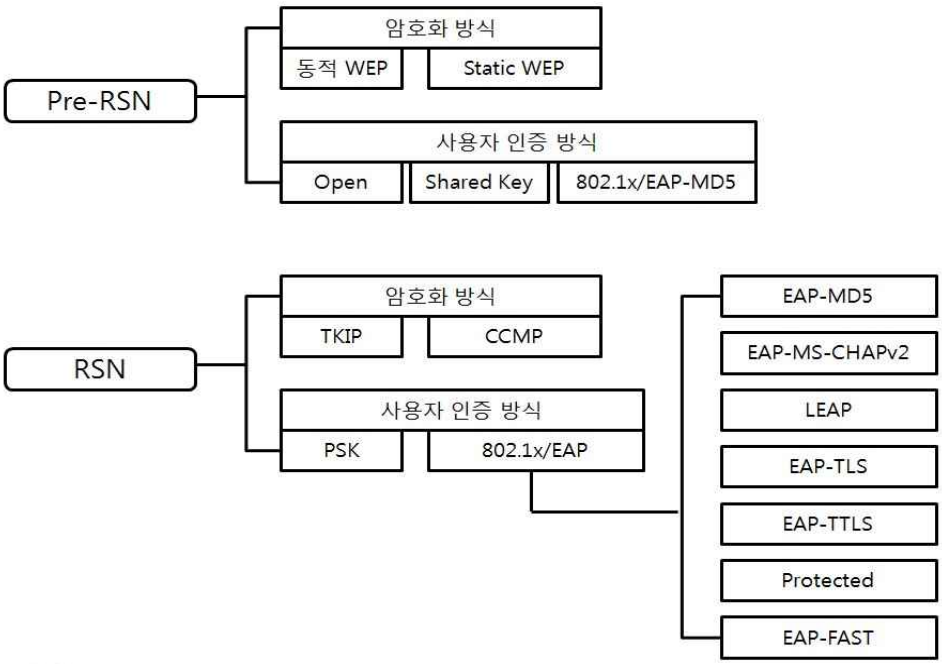


그림 5 Pre-RSN과 RSN

○ 2010년 현재 무선랜 보안 표준은 IEEE의 초기 802.11의 보안 표준인 WEP(Wired Equivalent Privacy)보다 크게 향상됐다. WEP은 공격받기 쉽고 벤더들에 의한 개선점이 빈약했었다. WEP의 결점으로 인해 802.11i 표준이 만들어졌으며, 이는 2005년에 승인됐다. 802.11i가 승인되기 이전에 WEP의 취약점을 보완하기 위해 와이파이 연맹은 WPA를 발표하였다. WPA는 RC4[9] 암호를 사용하는 TKIP(Temporal Key

9) Bit by bit로 평문 1비트에 키 1비트를 가지고 연산하는 알고리즘

Integrity Protocol)를 지원하는데, 기존장비에서 드라이버 또는 펌웨어 업데이트로 소프트웨어가 향상될 수 있었다. IEEE 802.11i가 표준화 되면서 개선된 망을 RSN(Robust Security Network)이라 하고 이전의 약한 보안 기법에 의한 802.11 무선 보안체계를 Pre-RSN이라 한다.

○ 무선랜 보안 표준

- WEP(Wired Equivalent Privacy)
  - 1997년 IEEE에서 정의한 보안 표준으로 인증과 암호화를 포함한 보안 프로토콜
  - 64비트의 키 길이를 가지는 고정키 방식의 인증 및 암호화
- WPA(Wi-Fi Protected Access)
  - 무선랜 장비간 호환성 시험을 위해 결성된 「와이파이 연맹」이 발표한 프로토콜
  - 이전의 WEP의 취약점에 대한 대안으로 나온 것으로 802.11i가 완성되기 전까지 일시적으로 사용하기 위해 개발
  - TKIP(Temporal Key Integrity Protocol)을 통해 데이터 암호화 향상
  - 동적 키교환(rekeying)기능 추가
  - MAC 주소 필터 기능이 추가
  - 802.1x/EAP(Extensible Authentication Protocol)을 통해 사용자 인증
- 802.11i(WPA2)
  - 2세대 WPA로서 보안 기능이 개선되었으며 AES(Advanced Encryption Standard) 암호화, 사전 인증 및 캐시로 구성

표 5 무선랜 인증 및 암호화

표준명	키분배방식	장비인증	사용자인증	암호화
OPEN	없음	없음	없음	없음
WEP	정적(공유키)	가능(약함)	공유키	RC4
WPA	정적(공유키) 동적(TKIP)	가능	802.1x	RC4
802.11i (WPA2)	정적(공유키) 동적(CCMP)	가능	802.1x	AES

○ 인증 방식

- OPEN

오픈 시스템은 글자 그대로 인증이 없는 경우(즉, Null Authentication)이다. 무선 전파 수신영역내의 모든 단말기기가 인증 없이 접속하여 사용하고 데이터는 암호화를 하지 않는 구성이다.

그림 6 Open 환경의 사용자 인증

- PSK(Pre Shared Key) 인증

사전에 AP(Access Point)와 무선랜 사용자가 특정 문자열을 패스워드로 공유하여 인증을 지원하는 방식이다. PSK 인증에서는 공유키를 통한

인증이 이루어지므로 공유키 관리가 매우 중요하다. WEP에서는 사용자 인증구조가 정의되어 있지 않다. 하지만 무선랜을 이용하기 위해 미리 공유된 키를 알고 있어야 하므로 사용자 인증의 일종이라 할 수 있다. 공유된 키를 통해 사용자 인증을 수행하고 해당키를 통해 암복호화를 진행한다.

그림 7 공유키 기반의 사용자 인증

- 802.1x/EAP 인증

EAP(Extensible Authentication Protocol) : IEEE 802.1x에서 사용자 인증을 위해 사용하는 프로토콜로서 확장성 필드를 이용하여, MD5, TLS, TTLS, SRP, FAST, PEAP, LEAP 등의 인증방식을 지원한다. 802.1x/EAP 인증은 사용자 인증을 위해 사용자 ID/Password를 사용하게 된다. 때문에 PSK와는 달리 사용자 Password를 관리하는게 매우 중요하다.

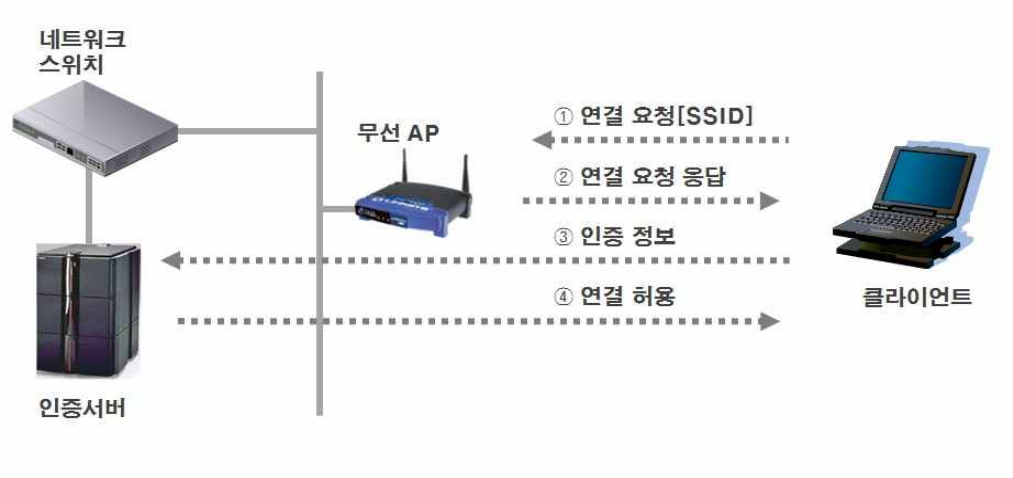
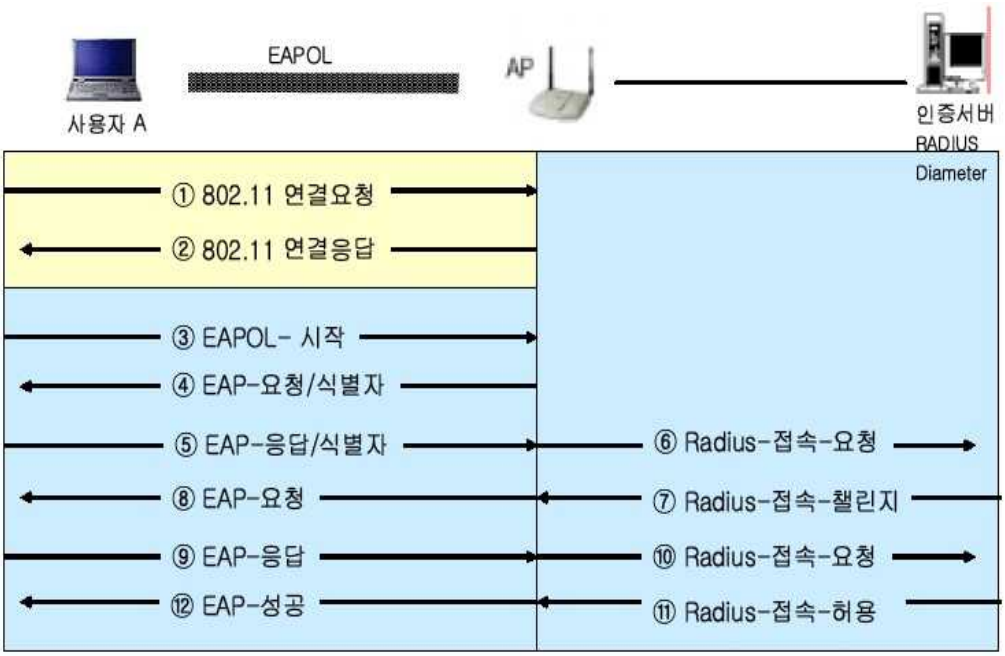


그림 8 인증서버 기반의 사용자 인증

- 802.1x 인증 메커니즘



출처 : 무선랜 안전운행 가이드

그림 9 EAP 인증 메커니즘

- 인증서버를 사용한 무선랜 접속

- 무선랜 단말기가 무선 AP와 네트워크 접속 시도,
- 무선 AP는 네트워크에 단말기가 인증이 될 때까지 단말기의 네트워크 접근시도를 차단
- 단말기의 사용자는 네트워크에 인증을 위해 인증정보를 입력
- 802.1x, EAP를 사용하여 무선랜 단말기와 유선랜에 연결되어 있는 인증서버가 상호인증을 수행
- 단말기와 인증서버의 상호인증이 성공적으로 완료되면 네트워크 접근을 위한 적당한 단말기의 수준을 정의하고 단말기를 구별할 수 있는 키를 결정
- 인증서버는 세션 키(Session-Key)를 유선랜에 위치한 무선 AP에 전송
- 무선 AP는 세션 키를 가지고 브로드캐스트 키를 암호화하여 단말기에 암호화된 키를 전송하며, 단말기는 암호화키를 복호화하기 위해 세션 키를 사용
- 단말기와 무선 AP는 세션의 유지 시간 동안 모든 통신에 세션과 브로드캐스트 키를 사용

○ 인증모드

- WPA-Personal

  인증서버를 사용하지 않고 PSK를 사용하는 방식으로 무선 AP와 무선 단말기가 동일한 키를 가지고 4웨이 핸드세이킹 절차를 통해 인증을 및 암호화를 수행한다.

- WPA-Enterprise

  인증서버를 사용하여 허가된 사용자에게 ID/Password 등을 통해 사용자 인증을 수행한 후 인증서버에서 생성한 키값을 정상적인 사용자에게 전송하고 암호화를 통해 데이터 전송을 수행한다.

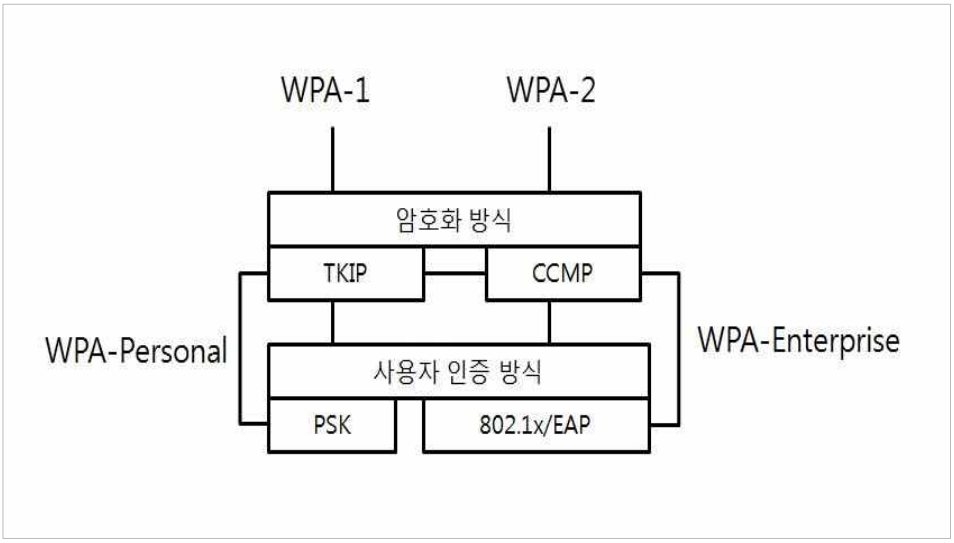


그림 10 인증모드의 구성

○ 암호화 방식

- Static WEP : 무선랜의 무선 구간에서 적용하기 위해 처음 제시된 대칭키 기반 암호화 기법으로, RC4 암호 알고리즘의 자체 취약성 및 키 노출 취약점을 내재
- Dynamic WEP : Static WEP의 키 노출 취약점을 보완하기 위하여 세션별 키를 변경할 수 있도록 보완한 무선랜 암호화 방식
- TKIP : WEP 과 동일한 RC4스트림 암호 방식을 사용하지만 각 프레임별로 시간별, 네트워크 세션별에 따라 상이한 키를 적용하고 필요한 경우 임시 비밀키를 자동으로 갱신함으로써 보안성을 강화 한 것이며 WEP의 암호화 방식을 소프트웨어를 통해 보완한 방식
  - 48bit 확장된 길이의 초기벡터 사용
  - 패킷마다 사용되는 암호키를 다르게 변경
- CCMP+AES : WPA의 필수 프로토콜인 TKIP를 대체하기 위해 만들어진 IEEE 802.11i(WPA2) 암호화 프로토콜로 WPA2 표준의 필수 요소이며, WPA 표준의 선택적 요소이고, AES(Advanced Encryption Standard) 알고리즘을

사용하는 일반인이 사용할 수 있는 가장 앞선 와이파이 보안 프로토콜
- 비밀성과 무결성을 위한 단일 암호키의 복잡도를 낮추며 성능 향상
- 패킷의 헤더와 데이터의 비밀성 및 무결성 보호

제3장

무선랜의 보안 위협

제 1 절 무선랜 보안위협

무선랜은 사용자들에게 유선에서 제공하지 못하는 이동성 및 접근성의 편리함을 제공해 주고 있다. 하지만 기업의 보안 관리자 및 사용자가 주의를 기울이지 않으면 본인도 모르게 선의의 피해자가 될 수 있으며 그 피해는 돌이킬 수 없을 지도 모른다. 3장에서는 무선랜이 가지는 보안 위협을 알아보고자 한다.

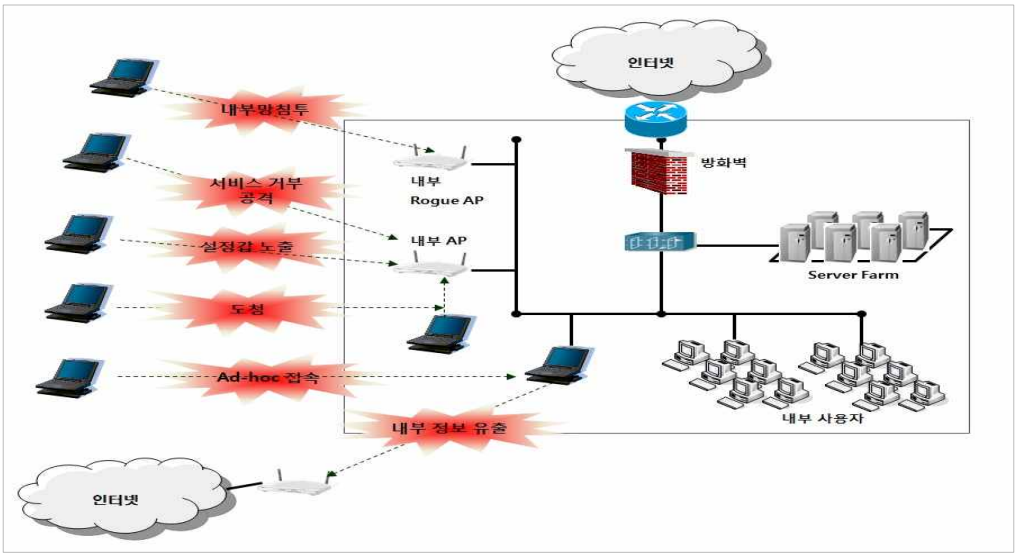


그림 11 무선랜 보안 위협

1. 내부망 침투에 대한 보안 위협

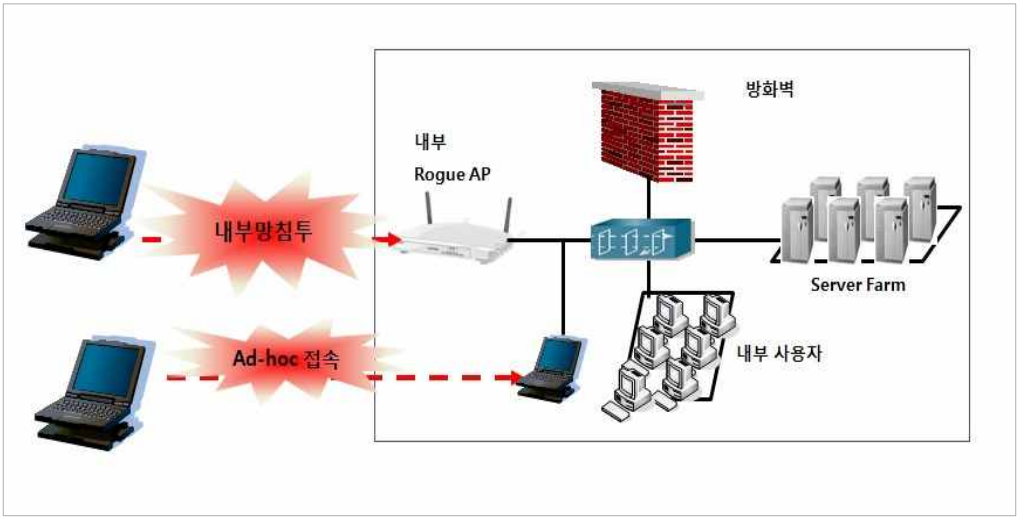


그림 12 내부망 침투에 대한 보안 위협

기업 내부망은 높은 보안성이 요구되는 구간으로 여러 보안장비와 정책에 의해 보호되고 있으며 외부와 독립된 폐쇄적인 환경으로 인해 기본적인 안정성과 신뢰성이 보장되고 있다. 그러나 업무 운영상 불가피하게 운영되는 사내 무선랜을 통해 잠재적인 보안위협 요소가 발생될 수 있다. 내부에 설치된 비인가 AP 또는 사용자의 잘못된 설정으로 인한 Ad-Hoc네트워크가 기업 네트워크의 백도어 역할을 하여 해당 위협 요소를 통해 불법 침입자가 내부 네트워크로 접근할 수 있다. 이런 침입자는 내부 직원과 같은 자격으로 모든 자원에 접속할 수 있게 되며 기업의 주요 서버 또는 기업의 중요한 자료에 접근하여 심각한 문제를 야기하게 된다. 내부의 비인가 무선 AP를 통한 우회 침투는 기업이 아무리 보안 시설에 투자를 했어도 한순간에 무용지물이 될 수 있다.

2. 내부정보 유출 위협

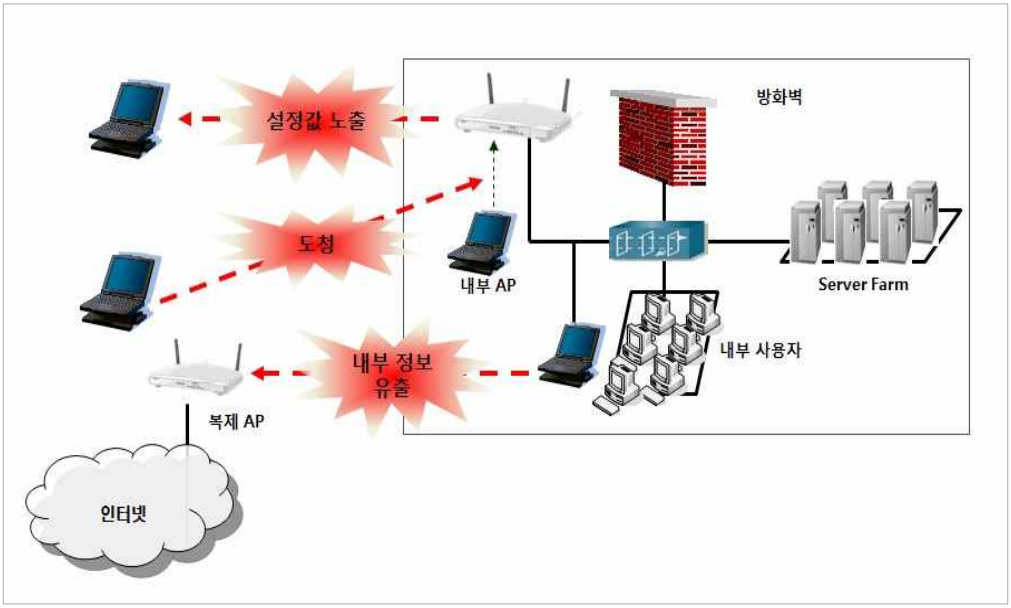


그림 13 내부정보 유출의 위협

무선 네트워크는 전파를 사용한다는 특성으로 인해 유선의 물리적인 연결이 필요하지 않다는 데서 취약점을 발생시킨다. 통신구간에 암호화가 적용되지 않아 통신되는 데이터가 도청되어 중요한 정보가 노출될 수 있다. 또한 미흡한 설정으로 인해 그 설정 정보가 노출되어 추가적인 공격과 내부 네트워크로의 접근에 이용될 수 있다. 외부에 내부의 무선 네트워크와 비슷한 무선 AP를 설치한 후, 내부 사용자에게 강한 전파를 전송시켜 내부사용자의 잘못된 접속을 통해 내부의 중요 정보가 유출될 수 있으며 내부 인가된 사용자가 인접한 외부의 무선 네트워크를 이용할 경우 기존의 보안정책을 우회하기 때문에 내부 보안 관리의 문제가 될 수 있다.

3. 서비스 거부에 대한 위협

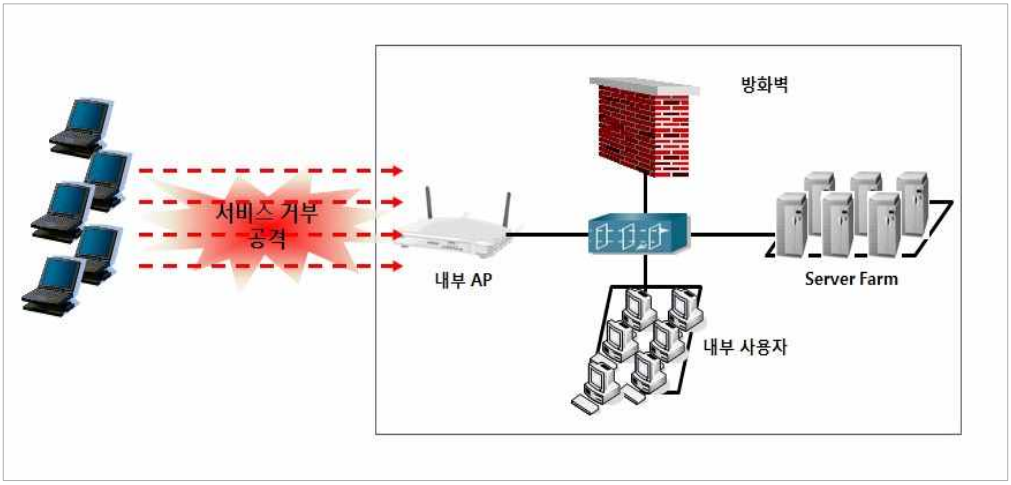


그림 14 서비스 거부에 대한 위협

서비스 거부 공격은 유선네트워크의 문제만이 아니다. 무선전파 수신 지역내에 있게 되면 무선 네트워크에 접속이 손쉬운 만큼 무선랜은 DoS 공격의 표적이 될 수 있다. 무선 네트워크에 대량의 무선 패킷 발송 및 접속 시도를 통해 서비스를 무력화 시키는 무선랜 DoS 공격은 실제로 내부 네트워크로의 침입이 시도되진 않지만 무선랜의 서비스에 장애를 일으켜 무선을 통해 실시간 업무가 이루어지는 곳에서는 업무에 커다란 문제를 일으킬 수 있다.

제 2 절 보안 취약점 발생 요인

1. 비인가 AP에 의한 위협

가. 비인가 AP(Rogue AP)를 통한 보안 위협

무선 AP는 유선네트워크와 무선을 연결하는 중계기 역할을 한다. 관리자의 인가를 득하지 않고 팀 또는 개인이 임의적으로 무선통신을 위해 조직 내부에 설치한 무선 AP는 모두 비인가 AP라 정의할 수 있다. 비인가 AP는 대부분 인증 및 암호화가 설정되어 있지 않거나 쉬운 보안설정으로 내부 네트워크에 연결되어 사용된다. 이렇게 내부 네트워크에 회사 내 보안 정책을 따르지 않고 일반 사용자가 개인적으로 설치한 무선 AP를 통해 외부의 비인가 사용자가 내부네트워크에 손쉽게 접속할 수 있다. 이때 추가적인 보안 대책이 존재하지 않을 경우 접속된 비인가자는 내부 직원과 같은 자격으로 모든 자원에 접속할 수 있게 된다.

비인가 AP는 그 종류가 매우 다양하다. 초기에는 무선 AP 장치만이 사용되었으나 현재는 소프트 AP, 가상소프트웨어 등을 비롯하여 3G를 무선 신호로 바꾸어 사용하는 와이파이 모뎀등 여러 가지 장치가 존재한다.

- 소프트 AP : 무선 인터페이스와 안전한 네트워크에 연결된 다른 인터페이스 간의 트래픽 전달 기능을 수행하는 노트북 또는 기타 무선 활성화 장치이다. 소프트 AP는 인터넷으로 연결되는 네트워크를 인가된 유선 이더넷 장치를 이용하므로 802.1x, NAC[10] 등과 같은

10) NAC : 기업내부의 네트워크에 엑세스 하는 모든 장비들을 포괄적으로 제어하고 보안위협으로부터 능동적으로 방어할수 있는 네트워크 접근 제어 솔루션

유선 측 보안 시스템을 우회하여 내부 네트워크 자원에 접속하게 된다.

- Windows 7의 가상 무선 AP : 특정 프로그램과 가상 무선 인터페이스 기능을 이용하여 한 개의 무선랜 디바이스가 무선 단말기로 동작하며 동시에 가상 무선 AP로 동작하여 무선인터넷을 공유하게 되어 내부 네트워크를 공유한다.

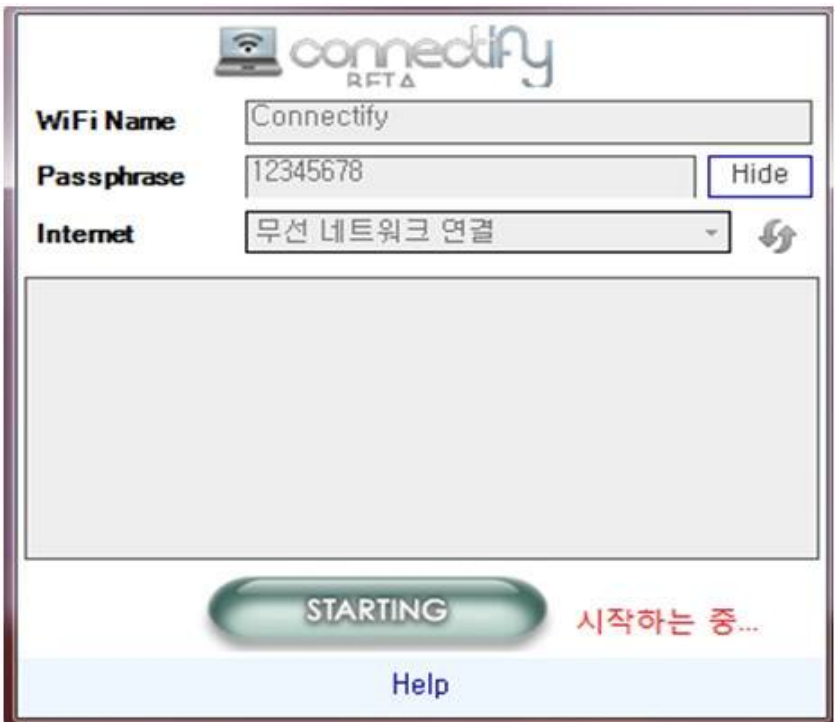


그림 15 가상 무선 AP 소프트웨어

- 스마트폰의 가상 소프트 AP : 테더링 기능을 통해 스마트폰이 무선 AP 역할을 하여 무선 네트워크를 사용할 수 있게 한다.

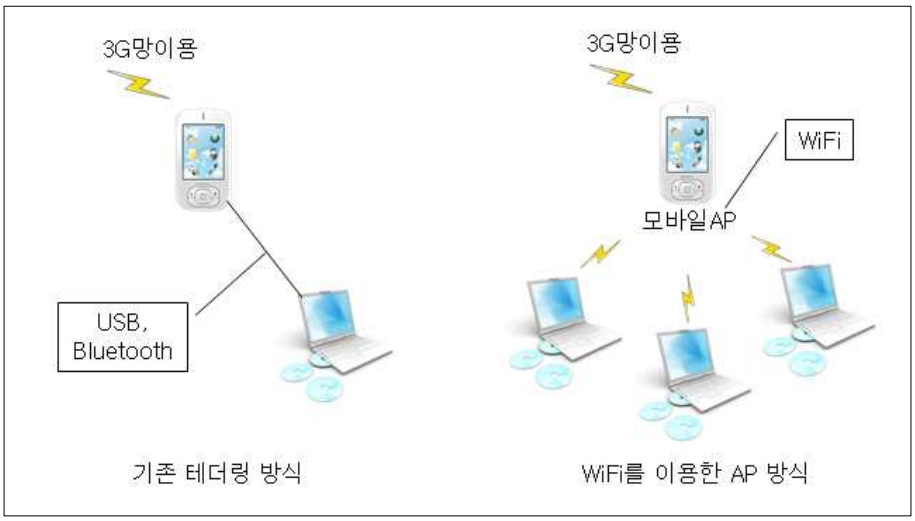


그림 16 기존 테더링과 모바일 AP 비교 그림

- 와이브로 Egg : KT의 Wibro 네트워크를 무선 신호로 변환하여 무선장비를 이용하게 하는 장치이다.

그림 17 Wibro 단말기 사진

나. Ad-Hoc 네트워크에 의한 보안 위협

Ad-Hoc 네트워크는 무선 통신에 일반적인 무선 AP를 사용하지 않고 단말기와 단말기간의 무선 네트워크를 이용하는 Peer to Peer 형식의 무선 네트워크를 말한다.
현재 802.11 a/b/g/n 기반의 무선랜 디바이스가 내장되어 있는 대부분의 노트북은 윈도우의 '무선 네트워크 설정'에서 누구나 손쉽게 Ad-Hoc 모드의 네트워크를 구성하여 별다른 추가 장치의 설치 없이 무선으로 여러 사람들과 개인적인 파일 혹은 중요한 업무용 자료 등 필요한 자료들을 서로 공유 할 수 있다. 이러한 Ad-Hoc 네트워크도 비인가 무선 네트워크와 동일하게 내부 네트워크로의 백도어 역할을 하는 위험이 존재한다.

2. 미흡한 무선랜 설정에 의한 취약점

비인가 AP로 인해 발생하는 문제도 있지만 내부의 인가된 AP 및 기본적인 보안설정 및 관리의 잘못으로 인해 발생하는 문제점도 많이 존재한다.

가. SSID의 미흡한 설정

❍ Default SSID 사용 : SSID는 무선랜 서비스 영역을 식별하기 위해 사용되는 ID이다. 무선 AP는 출고 시 기본적으로 해당 장비의 이름으로 설정되어 나온다. 이 설정 값을 변경하지 않고 그냥 사용할 경우 장비의 이름, 장비의 취약점 및 기본 설정 값을 확인하여 공격자는 공격에 이용할 수 있다. 또한 무선랜을 사용하는 기관의 명칭등을 SSID로 사용하게 될 경우에는 공격자의 공격 목표가 되어 위협을 받을 수가 있게 된다

○ SSID 브로드캐스트로 인한 AP 노출 : 무선 AP는 사용자의 접속을 편리하게 하기위해 SSID의 브로드캐스트가 기본적으로 설정 되어있다. 이 기능을 사용하게 되면 수신영역 안에 존재하는 모든 무선 단말기는 해당 무선 네트워크를 확인할 수 있다. 이로 인해 허가되지 않은 비인가자 및 불특정 다수가 네트워크에 접속을 시도하여 무선 AP의 자원을 소모하게 되거나 무선 AP가 안전하지 않은 인증 및 암호화 설정을 사용하는 경우 보안 위협에 노출될 수 있다.

나. 무선랜 서비스 전파 관리의 미흡

○ 무선 네트워크는 전파자원을 통해 접속한다. 이러한 전파가 수신되는 지역 내에 있는 단말기는 해당 무선 네트워크에 접속할 수 있는 가능성을 갖게 된다. 허가된 공간 이외의 장소에서 무선 네트워크가 검색 될 경우에는 비인가자의 접속 시도가 이루어지게 된다. 또한 무선 AP의 전파가 기업의 외부에서 탐지되면 공격자가 외부에서 내부 무선 네트워크로 공격을 시도할 수 있게 된다.

3. 관리자 접근통제의 부재

가. 관리자 접근통제의 부재

○ 무선 AP에는 무선서비스를 위해 사용자 인증 및 암호화 전파세기 및 네트워크 설정 등의 다양한 설정이 존재한다. 관리자는 이러한 설정을 관리하는 권한을 가지며 이를 위한 관리 설정 페이지가 존재한다. 이 관리자 페이지에 접속하게 될 경우 무선 AP에 대한 모든 권한을 가지게 된다. 관리자 페이지는 초기 사용자 편의를 위해 패스워드가 없

거나 기본패스워드로 설정되어 출고된다. 이 기본 패스워드는 장비의 종류와 버전별로 다르나 변경 없이 사용하거나 추측이 가능한 패스워드, 연속된 숫자로 된 패스워드 등을 사용할 경우 비인가자의 크래킹에 의한 무단 접속의 위협이 존재한다.

나. 물리적 접근 통제의 부재

○ 무선 AP는 원활한 서비스를 위해 일반적으로 외부에 노출되어 설치된다. 이로 인해 비인가자의 무선랜 장비에 손쉽게 접근할 수 있으며 장비 파손으로 인한 서비스 장애, Reset을 통한 설정의 변경으로 비인가자의 무단접속이 이루어져 내부 네트워크로의 접근이 이루어질 수 있다. 유선 구간에 연결된 네트워크를 우회시켜 정보 유출의 위협이 존재하며 실수에 의한 전원차단 및 유선의 제거 등으로 인해 실시간적으로 이루어지는 서비스에 영향을 끼칠 수 있다.

4. 안전하지 않은 암호화 및 인증

가. 암호화 및 인증

무선랜에 접속하기 위해서는 SSID 이외에 추가적으로 사용자 인증을 진행할 수 있다. 이때 취약한 인증 및 암호화 정책을 사용할 경우 중요정보가 도청되어 노출되거나 인증키 해독을 통한 비인가자의 접속이 시도될 수 있다.

○ OPEN

무선 전파 수신영역내의 모든 단말기기가 인증 없이 접속하여 사용

하고 데이터는 암호화를 하지 않는 구성이다. 이러한 구성의 장점은 네트워크 성능이 가장 좋으며 사용자가 구성하고 사용하기에 가장 편리하다는 데 있다. 대부분의 경우 장비의 기본 셋팅만으로도 동작을 하며 사용자는 IP 주소만 설정해 주면 된다. 하지만 인증 및 암호화가 없어 도청 및 비인가자의 접속에 따른 위협이 존재한다.

❍ PSK(Pre Shared Key) 인증 및 암호화

- WEP 인증 및 암호화 취약점

  사용자가 AP에 접속 시 미리 설정한 WEP 키를 알아야만 인증을 하도록 하는 방법이다. 무선 구간에서 전송되는 데이터패킷을 RC4 스트림 암호 방식을 이용하여 MAC 프레임에 대한 암호화를 수행한다. 쌍방간에 미리 결정된 40bit 또는 104bit 길이의 WEP 키와 초기화 벡터(IV)를 이용하여 연속된 키 스트림을 생성하고 이것을 전송할 평문과 XOR(exclusive OR)연산을 수행하여 암호문을 생성하는 방식이다. WEP는 데이터의 암호화를 진행하며 스트림 암호화 특성상 속도가 빠르고 구조가 간단하다.

  하지만 WEP는 보안상에 몇 가지 문제점이 있다. 그 중에서도 취약한 IV의 문제점이 있으며 이 취약한 IV 문제점을 이용한 FMS(Fluhrer, Mantin, Shamir) 공격 기법은 현재까지 알려진 가장 효율적인 방법이다.

  FMS 공격은 WEP 공격에 가장 많이 쓰이는 방법으로 RC4의 키 스케줄링 알고리즘과 IV 사용법의 약점을 이용한 방법이다. IV값 중에는 키스트림의 첫번째 바이트에 비밀키에 대한 정보를 노출시키는 취약한 IV가 있다. 패킷을 암호화할 때 IV는 계속 바뀌지만 이 비밀키는 바뀌지 않고 그대로 계속 쓰인다. 취약한 IV를 사용하는 충분한 패킷을 수집했다면 추가적인 작업을 통해 비밀키를 알아낼 수 있다. 인터넷에서 쉽게 구할 수 있는 툴로 10분 정도의 패킷수집 과정을 거치게 되면

WEP의 공유키는 쉽게 노출된다.

이를 보완하기 위해 동적 WEP키를 짧은 주기로 변경하는 동적 WEP이 존재한다. 동적 WEP 암호화 방식은 암호화키 크랙을 방어하는 방법이기는 하지만 키 크랙을 완벽하게 방어할 수는 없다.

이렇게 WEP 알고리즘은 IV의 평문전송, 키 스트림의 단순성, 고정키 사용에 따른 RC4 키 갱신 부재 등으로 인해 키 길이에 상관없이 그 보안기능이 취약하다.

○ WPA-PSK 인증 및 암호화

128비트 암호화방식을 취한 WPA방식은 보다 확장된 데이터 암호화(TKIP: Temporal Key Integrity Protocol)를 사용자 인증 기능을 통해 제공하고 있다. 대칭벡터라 불리는 WEP 헤더의 취약점(고정 암호키 방식)을 해결하기 위해 그 대응책으로 개발되었다.데이터 암호화를 강화하기 위해 순서 규칙이 있는 48비트 초기화 벡터(WEP에서는 24비트 초기화 벡터)를 이용하는 TKIP(Temporal Key Integrity Protocol)과 AES(Advanced Encryption Standard) IEEE 802.11i 보안 표준을 사용한다. 즉, 무선 통신상의 전송내용을 암호화하는 암호키가 기존 WEP에서는 고정되어 있던 것과 달리, WPA는 암호키를 특정 시간이나 일정 크기의 패킷 전송 후에 자동으로 변경시키기 위해 개발된 것이다.

하지만 WPA에 사용되는 TKIP 역시 WEP을 기반으로 하면서 여전히 RC4 알고리즘을 사용하고 있고 키 관리 방법을 제공하지 않는다. 정해진 시간동안은 공유된 키를 사용한다는데 있어서 WEP의 크랙 공격 가능성을 내재하고 있으며 WEP이 갖고 있는 기본 취약성을 그대로 갖고 있다. 또한 기존 WEP의 소프트웨어 업그레이드를 통해 소프트웨어적으로 암호 및 인증을 처리하고 있어 속도 저하와 암•복호화로 인한 시간지연의 문제가 존재한다.

PSK 인증 방식은 미리 공유된 키를 통해 접속되는 방식으로 사전(Dictionary) 공격을 방어하는 수단이 갖춰져 있지 않다.

❍ WPA "Hole 196" 취약점

이론적으로 가장 안전하다고 알려진 WPA2에도 “Hole 196”이란 취약점이 존재한다. IEEE 802.11 표준(개정, 2007)의 1,232페이지 중에서 196페이지에서 밝혀진 취약점이라 하여 붙여진 이름이다. 인증(PSK 또는 802.1x) 및 암호화(AES)와 관계없이 모든 무선 네트워크의 WPA/WPA2 사용자는 이 취약점을 가지게 된다. Hole 196 취약점은 악의적인 내부 사용자가 네트워크상에 인가된 다른 무선랜 사용자에게 직접 그룹 공유 키(GTK)를 사용하는 암호화된 변조된 패킷을 보내고, AP를 통해 내부 사용자가 그들의 데이터를 리다이렉션하여 인가된 사용자를 차례로 속이는 방법이다. 이 취약점은 제한된 내부 사용자에 의한 공격으로 암호화 키의 크랙 등은 포함되지 않는다.

제4장

무선랜 구축시 보안 고려사항

3장에서 언급하였듯이 무선랜은 그 특성상 몇 가지 취약점이 존재한다. 본 장에서는 무선랜을 설치하고 운영시 적용하여야 할 보안설정 및 고려사항에 대해 기술한다.

제 1 절 기술적 위협 대응 방안

무선랜의 안전한 운영을 위해서는 몇 가지 고려사항이 존재한다. 유선랜과 무선랜 구간의 구분, 전송데이터의 보안, 접근제어, 서비스거리 제한 등과 같은 사항에 대해서 기준을 설정하게 되면 무선랜의 보안이 향상될 수 있다.

본 절에서는 안전한 무선랜의 설정을 위한 기술적인 부분에 대해서 기술한다.

1. 기본 설정 변경

○ 무선 네트워크를 위해 구성되는 무선 AP가 출고될 경우, 기본적으로 설정된 값인 SSID, 관리자 페이지의 ID/Password, 전파 세기 등의 설정 값을 강화하여 사용하여야 한다. 무선 네트워크의 기본설정의 강화만으로도 3장에 나열된 보안 위협을 보완하고 무선 네트워크를 보다 안전하게 이용할 수 있게 된다.

가. SSID 설정

○ SSID는 가장 먼저 무선 네트워크를 구분하는 ID값이다. 이 SSID값을 무선랜 서비스를 제공하는 기관의 이름이나 부서를 추측할 수 있는 값으로 설정하지 않고 무선 AP의 장비명을 추측할 수 없도록 설정한다.

○ SSID를 숨김모드를 사용하면 SSID를 모르는 사용자일 경우 자신이 위치한 곳에서 제공되는 무선랜 서비스가 없기 때문에 무선랜 서비스에 접속할 수 없게 된다. 인가된 사용자에게 미리 SSID를 알려주어 접속하도록 하면 비인가자의 접속시도를 줄일 수 있다. 물론 특정 프로그램을 사용하게 되면 SSID를 알 수 있지만 일정시간 무선데이터를 수집하고 분석하는 불편함을 줄 수 있는 최소한의 접근제어 방법이다.

나. 관리자 페이지에 대한 접근제어

○ 장비의 출고시 초기 관리자의 ID/Password는 설정되어 있지 않거나 쉽게 설정되어 있으며 이는 암호화 설정을 하지 않은 보안수준으로써, 반드시 통용되는 수준의 암호설정을 통해 무선 AP를 관리•운영하도록 한다.

표 6 안전한 무선 AP 관리 암호의 예

안전한 무선 AP관리암호 사용 예
- 8자 이상의 암호 사용
- 숫자 및 영문자, 특수문자 혼용사용
- 일반 단어가 아닌 한글-영타암호 사용
- 주기적인 암호의 변경

○ 비인가자의 접속을 통한 네트워크 설정 변경 및 중요 정보가 노출

될 위험이 존재하므로 허가된 장비에서만 관리자 페이지에 접근이 가능하도록 고정IP와 고유하게 부여된 MAC 주소로 접근 제어를 수행한다.

다. 무선랜 전파출력 조절

○ 인가된 내부 사용자만 접속할 수 있도록 무선랜 전파세기를 조절하여 인가된 공간 외에서 무선랜의 전파가 탐지되지 않도록 한다.

라. MAC 필터링

○ 각각의 무선단말장치에 부여되는 고유한 번호(MAC)를 통해 사용자 인증을 하는 방식이다. 접속을 허용하는 사용자의 단말기 MAC을 사전에 등록하고 등록된 장비 접속을 허용한다. 하지만 무선랜에 대한 도청을 통해 인가된 무선단말장치의 번호를 수집 후 비인가된 장치의 MAC을 변조하여 접속을 시도하게 되는 위협이 존재하므로 추가적인 보안대책이 필요하다.

마. 인증 및 암호화의 변경

○ 인증 및 암호화는 무선 네트워크의 접근 및 정보를 보호하는 가장 중요한 매체이다. “3. 사용자 인증 및 데이터 암호화”를 참조하여 기본으로 설정된 값의 변경 후 무선랜을 사용하도록 한다.

2. 무선랜의 고정 IP 사용 및 유·무선 네트워크 분리

○ 무선 접속에 관련된 키 값이 노출되었을 경우 비인가자가 노출된

키를 통해 무선 네트워크에 접속 할 수 있게 된다. 이때 DHCP 서비스가 활성화 되어 있다면 비인가자 단말기는 자동으로 내부의 IP를 할당받아 내부 네트워크에 접속 하게 된다. 이를 방지하기 위해 무선 AP에서 DHCP 서비스를 사용하지 않고 고정 IP를 사용하여 접속하도록 강화한다.

○ 기존의 유선 네트워크와 무선 네트워크가 동일한 구간을 사용할 경우 무선랜의 취약점을 통한 침해사고 발생시 그 피해는 전사적으로 확산될 가능성이 있다. 유선랜과 무선랜이 사용되는 네트워크를 구분하고 무선랜의 사용범위를 구분하여 침해사고 발생시 피해규모와 피해의 확산을 제한된 범위로 한정할 수 있도록 한다.

3. 사용자 인증 및 데이터 암호화

무선랜 장비에서 기본적으로 제공하는 보안 체계인 WEP를 사용한다는 것은 무선랜 보안을 하지 않은 것과 동일한 일이다. 또한 PSK(Pre-Shared Key) 인증도 안전하지 않는 방법이다. 가장 강력한 사용자 인증, 암호화 방식을 사용하고 802.1x EAP 인증 방식을 이용하여 유·무선랜 장비를 연동시켜 안전하게 무선랜을 이용하도록 하여야 한다.

가. 무선랜 사용자 인증

○ 802.1x EAP 사용자 인증

802.1x 인증은 WPA나 WPA2 방식 둘 다 동일하게 다양한 인증방식을 사용할 수 있다. WPA와 WPA2는 개인과 기업 등 2개의 인증 방식을 포함한다. WPA-PSK은 PSK 또는 사전 공유키로 불리는 평범한 텍

스트 통과 문구(plain-text pass phrase)로부터 256비트 키를 생성한다. 하지만 PSK는 사전에 공유된 키 값을 동일하게 갖는다는 점으로 인해 키 노출의 문제점을 가지고 있다.

반면 WPA-Enterprise는 정적인 키를 관리하고 분산시키는 것에 대해 인증 서비스에 접근함으로써 계정을 기반으로 접속하게 된다. 사용자 이름과 암호 또는 인증서나 일회용 암호 등과 같은 자격을 요구하고, 인증은 인증서버와 무선 사용자 사이에서 이뤄진다.

- 주요 구성요소

802.1x 인증의 주요 구성요소는 인증서버, 무선 AP, 단말기 3 가지이다. 인증서버에서 키를 생성해 인증서나 ID/Password를 기반으로 사용자를 상호인증하고 무선구간의 통신 데이터를 암호화 할 수 있도록 제공하며, 암호화 키를 안전하게 관리하는 기능을 수행한다. 인증 솔루션은 인증(Authentication), 권한관리(Authorization), 통계(Accounting)라는 AAA서버[11]를 지원하는 것이 필수 사항이며, 무선 네트워크의 서비스에 큰 영향을 미치기 때문에 안정성과 처리 성능이 가장 중요하다. EAP 구성에서 무선 AP는 단말기로부터 EAP 트래픽을 받게 될 때, 인증서버로 이를 건네는 중계기 역할을 수행한다.

- 802.1x 구축시 고려사항

WPA-Enterprise를 적용하기 위해서는 반드시 IEEE 802.1x를 이용해야 한다. 더불어 유무선랜에 대한 통합 인증, 인사시스템(RDBMS, LDAP, Active Directory 등)과의 연동을 통한 휴면 계정 최소화 및 인증체계의 일원화를 고려해야 한다.

EAP 사용자 인증 방식에는 인증서를 사용하거나 마이크로소프트 윈도우 운영체제에서 지원하는 기술을 이용해 ID/Password로 인증을 처

11) AAA서버 : 인증, 권한부여 및 회계 서비스를 제공하는 서버

리할 수 있는 TLS(Transport Layer Security), TTLS(Tunneled Transport Layer Security), PEAP(Protected Extensible Authentication Protocol)이 있다. 모두 무선랜 장비에서 지원하고 있으며, 각 사의 사용자 환경과 보안정책에 맞게 적절한 인증 방식을 선택할 수 있다.

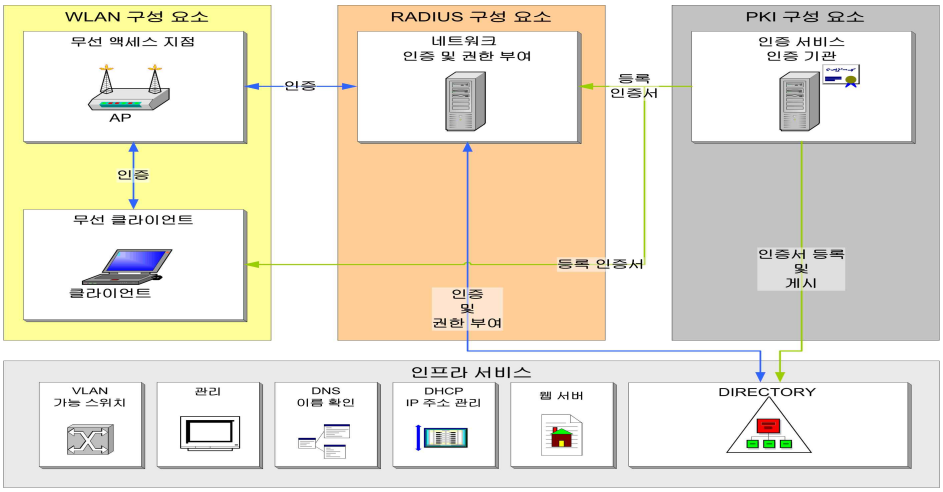


그림 18 802.1x 인증서버 환경의 구성

나. 무선랜 데이터 암호화

- WPA의 TKIP, CCMP 기술은 크래킹이 가능한 기존의 WEP보다 보안성이 높으며, WPA2의 AES를 사용하는 CCMP가 가장 높은 보안 수준을 제공하는 것으로 알려져 있고 IEEE에서도 WPA2(AES)를 무선랜 표준으로 정의하였다.

  Wi-Fi 연합은 WPA의 TKIP만을 정의하며 AES에 대해서는 정의되지 않고 IEEE 802.11i에서는 WPA2의 AES만을 정의하고 있으나 기존장비와의 호환성을 위해서 TKIP, AES를 모두 지원하였다. 하지만 최근에는 WPA, WPA2 모두 TKIP, AES를 지원한다. 그러나 WPA에서 AES 알고리즘을 사용하는 방식은 IEEE에서 테스트 되지 않고 정식 인증되지 못한 방식으로 WPA2수준의 보안성을 제공해 주지는 못한다.

또한 WPA2에서도 TKIP 알고리즘을 사용할 수 있지만 TKIP의 RC4 암호화 알고리즘이 가지는 취약점으로 인해 강화된 WPA2의 잇점이 사라진다.

WPA2는 AES의 기반으로 CCMP라고 불리는 새로운 암호화 방법을 사용하여 무선 네트워크의 기밀성과 데이터 무결성을 보장한다. 때문에 특수한 경우를 제외하고는 WPA2(AES) 암호화 알고리즘을 통해 무선 네트워크의 데이터를 보호하여야 한다.

제 2 절 관리적 위협 대응 방안

1. 무선랜 운영을 위한 관리 지침

❍ 무선랜 설치 전에 사용 목적 및 올바른 운영방향을 지정하여야 한다. 무선랜의 서비스 범위와 용도를 지정하고 서비스 시간 및 사용자 절차 등 무선랜에 관련된 일련의 사항들을 미리 정의하여 설치, 운영, 감사의 모든 분야를 포함하는 무선랜 관리지침을 통해 안전한 무선 네트워크를 운영한다.

- 무선랜의 용도 및 사용 범위 지정
  무선랜의 사용 용도와 용도에 따른 범위를 지정하여 무선랜의 전파 세기 등을 조절하고 사용자를 한정한다.
- 무선 장비(AP 및 무선단말장비) 및 사용자 현황 파악
  무선 장비의 설치 리스트 및 무선단말기, 사용자 정보를 파악하여 일반적인 관리를 진행하고, 추가적으로 무선랜의 접근 통제시 이를 바탕으로 무선장비의 관리를 진행한다.
- 무선랜 구성도
  무선랜을 통한 네트워크 구성도를 구비하여 장애처리 및 무선랜을 통한 데이터의 흐름을 통제하고 사고발생시 신속한 원인을 찾는데 도움이 되도록 한다.
- 암호 변경의 주기
  무선장비의 보안을 강화하기 위해 관리자 암호 및 AP의 인증 암호 등을 일정수준 이상의 보안이 유지되도록 변경주기 및 암호정책을

정의한다.

- 무선랜의 사용절차
  무선랜에 대한 등록, 접속, 폐기 등의 일련에 대한 절차를 정의하여 사용자의 편의를 제공한다.
- 무선랜의 관리 담당자
  무선랜의 설치 운영을 위해 담당자를 지정하여 주기적인 점검 및 장애 발생시의 전반적인 운영관리를 진행한다.
- 무선랜의 보안점검

- 무선랜의 정기적인 보안점검을 명시하고 보안점검의 실시 항목을 정의하여 무선랜의 보안상태를 주기적으로 점검하는 정책을 수립한다.
- 비인가 AP를 방지하기 위해서는 관리자가 분석기를 가지고 AP 도달거리 범위를 돌아다니며 탐지하는 등의 직접적이고 물리적인 감시가 최선이다.

- 로그 데이터 관리
  무선 AP, 인증서버 등 무선랜에 필요한 장치들에 대해 주기적으로 로그 점검을 실시하고 불법행위의 여부에 대한 정책을 정의한다.
- 무선랜의 설정 정의
  무선랜의 운영을 위한 위치별, 장비별 등의 특성에 따른 보안설정 및 암호화, 인증 등에 대한 전반적인 설정을 정의하여 관리한다.

표 7 무선랜 구축 및 운영단계의 고려사항

구 분	내 용
계 획	- 무선랜의 필요성 정의 - 무선랜의 용도 정의, 사용 범위 지정 - 인증 및 암호화 설정 정의 - 무선랜 사용절차 정의 - 암호 및 변경주기 등에 대한 정의 - 무선랜 보안 체크리스트 정의
운 영	- 계획에 따른 설정값을 통한 일괄 설정 - 무선랜 사용자 및 단말기 등 리스트 관리 - 주기적인 무선랜 사용자 관리 - 로그 데이터 관리 - 무선랜을 포함한 네트워크 구성도 관리
감 사	- 주기적인 비인가 AP 탐지 및 제거 - 체크리스트에 따른 무선랜 점검

2. 무선랜 보안 교육

❍ 무선랜의 보안은 시스템의 보안과 관리자만의 노력으로 유지될 수는 없다. 보안담당자가 정의한 정책을 사용자가 지키지 않고 보안정책을 알지 못한 사용자의 실수로 인해 설치된 비인가 AP가 전체적인 네트워크에 치명적인 영향을 줄 수도 있다. 때문에 직원을 대상으로 무선랜에 대한 이해와 보안의 필요성, 올바른 사용법을 포함 보안교육을 주기적으로 실시하여 보안의식 수준을 향상시켜 안전하고 편리한 무선 네트워크 이용이 되도록 하여야 한다.

3. 물리적 통제

○ 물리적인 접근통제를 사용하여 무선랜의 운영측면의 보안 대책을 수립할 수 있다. 물리적인 방법은 무선 네트워크 지원시설에 대해 접근통제대책을 수립하는 것으로 사용자의 카드키, 서명, 지문인식 통제 등을 사용하여 비인가자의 무선랜 설비에 대한 접근을 방지할 수 있다. 또한 잠금장치 폐쇄회로(CCTV) 등을 사용해 무선랜 장비 및 관련시설의 불법적인 접근을 감시할 수 있다.

4. 무선랜 보안 솔루션

○ 무선랜 환경에서는 인증·암호화 등의 기술적인 보완을 통해서 차단할 수 없는 다수의 위협이 존재한다.

○ 내부 네트워크에 연결된 장소에서 비인가 무선랜이 설치되고 Ad-Hoc 네트워크 무선랜이 운영 중일 경우 외부 사용자가 내부 네트워크로 접속할 가능성이 존재하므로 주기적인 점검 또는 무선랜 정보보호 시스템 도입을 통해 이런 위협요인의 차단대책을 강구하여야 한다.

제 3 절 무선랜 구성의 예

1. 인증서버를 사용한 무선 네트워크 운영

표 8 Enterprise 환경에서의 무선랜 구축 정책의 예

구 분	적 용 방 법	비 고
사용자 인증	o 인증서버 인증	
데이터 암호화	o Dynamic WEP(1분주기)	
	o WPA2(AES),	
IP설정	o 고정 IP 설정	
전파관리	o 특정 공간만으로 전파 조절	

○ 대규모 네트워크에서는 IEEE 802.11i에서 정의한 802.1x EAP 인증방식을 적용한 WPA-Enterprise방식을 적용한다. 이를 위해서 인증서버를 필수적으로 설치하고, 무선 사용자의 인증을 관리하고 비인가 사용자의 접속을 차단한다.

○ 검증된 암호화 기법인 AES를 기반으로 무선랜 환경의 데이터에 대한 비밀성과 무결성을 보장하며 IEEE 802.11i의 표준을 따르는 전송 데이터의 암호화기법인 CCMP를 사용한다.

○ 하드웨어가 지원하지 않아 WPA2를 사용하지 못하는 경우에는 1분의 키 변경 주기를 가진 Dynamic WEP를 사용하여 암호화 키값이 노출되지 않도록 한다. 하지만 Dynamic WEP를 사용하여 운영할 경우

관리 패킷의 증가로 인해 AP의 사용자 데이터 전송률이 저하되는 경우가 발생하므로 구축시 고려하여야 한다.

○ 무선랜 사용자를 조사하여 해당 사용자들에 대한 IP를 고정으로 할당하여 사용하도록 한다.

○ 또한 아래와 같은 다양한 인증방식이 제공되므로 기관에 적합한 인증방식을 채택하여 적용한다.

표 9 인증방식에 따른 보안방식

구 분	MD5	TLS	TTLS	PEAP	LEAP
단말기측 인증서	아니오	예	아니오	아니오	아니오
서버측 인증서	아니오	예	예	예	예
WEP 키 관리	아니오	예	예	예	예
비인가 AP 감지	아니오	아니오	아니오	아니오	예
인증 속성	일방	쌍방	쌍방	쌍방	쌍방
구축 난이도	용이	난해	중간	중간	중간
무선 보안	불량	최고	고급	고급	고급

출처 : http://support.intel.com/support/kr/wireless/wlan/sb/cs-008413.htm

○ 대규모 네트워크의 무선랜 구성 예

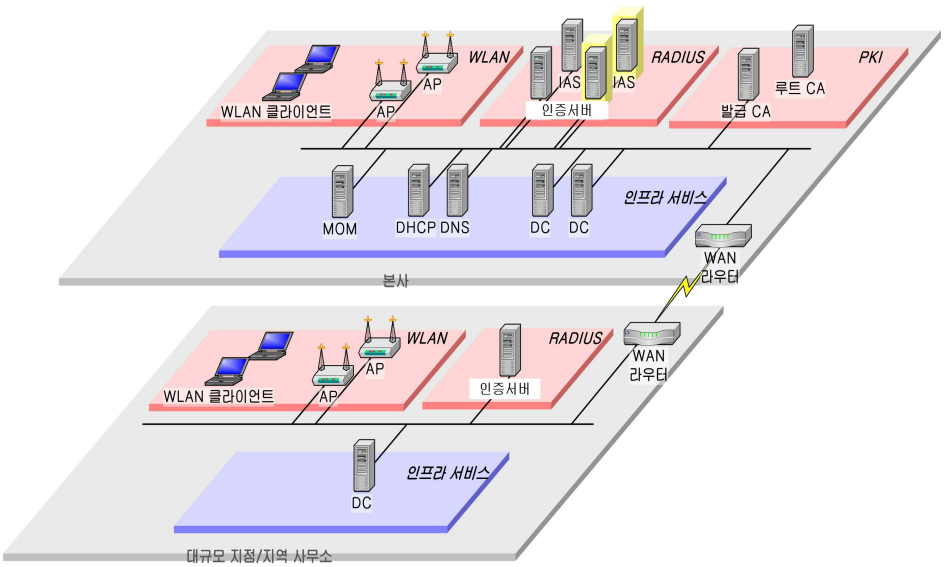


그림 19 WPA2(AES) 및 EAP-TLS를 이용한 무선랜 구축의 예

2. 인증서버를 사용하지 않는 무선 네트워크 운영

이 구성은 인증서버를 사용하지 않는 무선 네트워크 구성에 대한 예이다. 이러한 네트워크는 외주 개발환경, 회의실 등의 특수한 장소에서 필요한 경우에만 사용하도록 하여야 한다. 공유된 키를 사용하여 키 노출에 대한 위협이 존재하므로 사용자 인증 후에도 중요한 네트워크로 접속을 차단하고 특정 포트만을 사용하도록 제한하는 등 2차적인 보안이 필수적으로 동반되어야 한다. 또한 해당 무선 네트워크상에 중요한 데이터가 사용되지 않도록 사용자의 보안교육도 반드시 필요하다.

표 10 Personal 환경에서의 무선랜 구축 정책의 예

구 분	적 용 방 법	비 고
사용자 인증	o Pre Shared Key 인증	
데이터 암호화	o WPA1/2(AES),	
사용자 접근제어	o MAC 필터	
IP설정	o 고정 IP 설정	
전파관리	o 특정 공간만으로 전파 조절	

○ SSID를 숨김모드로 설정하여 허가되지 않은 사용자들의 접근을 제한하고 SSID를 장비명, 회사명 등으로 설정하지 않도록 하여 공격 목표가 되지 않도록 설정한다.

○ WPA-PSK(Wi-Fi Protected Access - Pre Shared Key) 사용

- WPA-PSK는 개인사용자를 위한 WPA의 기술이며 일반적으로 WPA-Enterprise기술이 권장되지만, 인증서버를 두기 어려운 상황에서 사용하기를 권고한다.
- WPA-PSK TKIP은 WEP키 암호화 알고리즘의 취약점이 상존하고 있으므로 TKIP암호화 대신 AES로써 보다 강력한 암호화를 사용하고 최대한의 자리수로 키를 설정하여 사용하도록 한다

○ MAC 주소 변조를 통해 우회 접속이 가능하나 서비스지역을 지정하고 사용지역의 무선 AP에만 MAC주소를 등록하여 지정장소 이외에서는 무선 단말기가 통신이 되지 않도록 조치하여 사용한다.

○ 무선 AP의 DHCP 서비스를 비활성화 하고 사용자별로 IP를 고정으로 지정하여 사용하도록 한다.

○ 사용부서 및 용도별로 무선랜의 전파를 조절하여 특정 공간에서만

무선 네트워크를 사용할 수 있도록 한정하며 무선 네트워크 구간을 기존의 유선 네트워크 구간과 별도로 관리하여 접속구간을 제한한다.

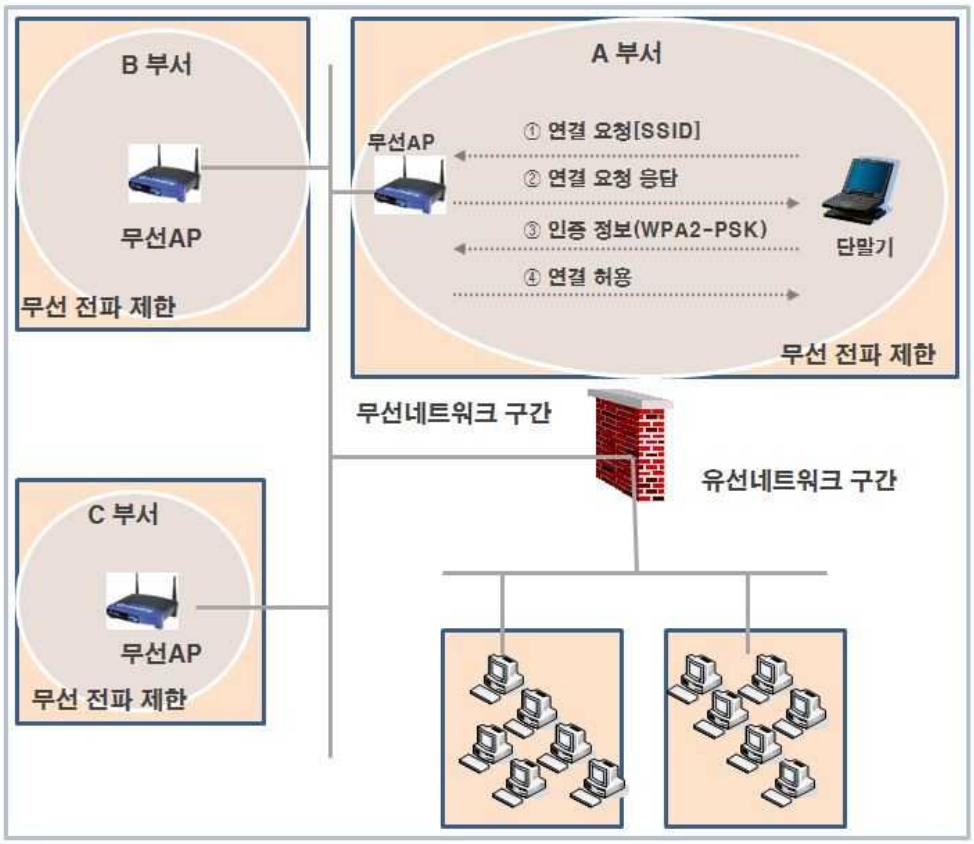


그림 20 Personal 환경에서의 무선랜 구축의 예

3. 고객서비스를 위한 무선 네트워크 구성

표 11 고객 서비스용 무선랜 구축 정책의 예

구 분	적 용 방 법	비 고
사용자 인증	o Pre Shared Key 인증	
데이터 암호화	o WPA1/2(TKIP, AES),	

❍ 최근 ISP에서 제공하는 무선 장치를 이용하여 고객 서비스용 무선랜을 설치하는 기관들이 늘어나고 있다. 이때 고객 서비스용 무선랜은 해당 기관에서 제공하는 것으로 인식이 되어 보안사고 발생시 금융기관에 피해보상에 대한 문제가 발생할 수 있다. 고객용 무선랜 서비스 제공 시 무선 통신 데이터에 대해 암호화를 필수화하여 서비스 이용 고객의 개인정보를 포함한 무선통신 데이터가 도청되는 사고를 예방함으로써, 안전하지 않은 무선랜 제공으로 인한 도덕적, 사회적 책임 소재가 해당 각 기관으로 전가되어 브랜드의 이미지에 영향을 받지 않도록 해야 할 것이다.

❍ WPA-PSK(Wi-Fi Protected Access - Pre Shared Key) 사용

- 무선랜 서비스의 제공에 대하여 사용자가 인식할 수 있도록 눈에 띄는 곳에 무선랜 사용자 인증키를 부착하고 개별 프레임, 개별 사용자별로 세션키를 다르게 제공하는 AES 암호화키를 사용한다. 일부 단말기에서 AES암호화 알고리즘을 지원하지 않아 TKIP을 사용할 수 있으나 WEP키 암호화 알고리즘의 취약점으로 인해 암호 해독의 가능성이 있으므로 TKIP 적용시에는 무선랜 데이터 사용시 데이터 보호에 대한 책임의 여부를 사전에 공지하여야 한다.

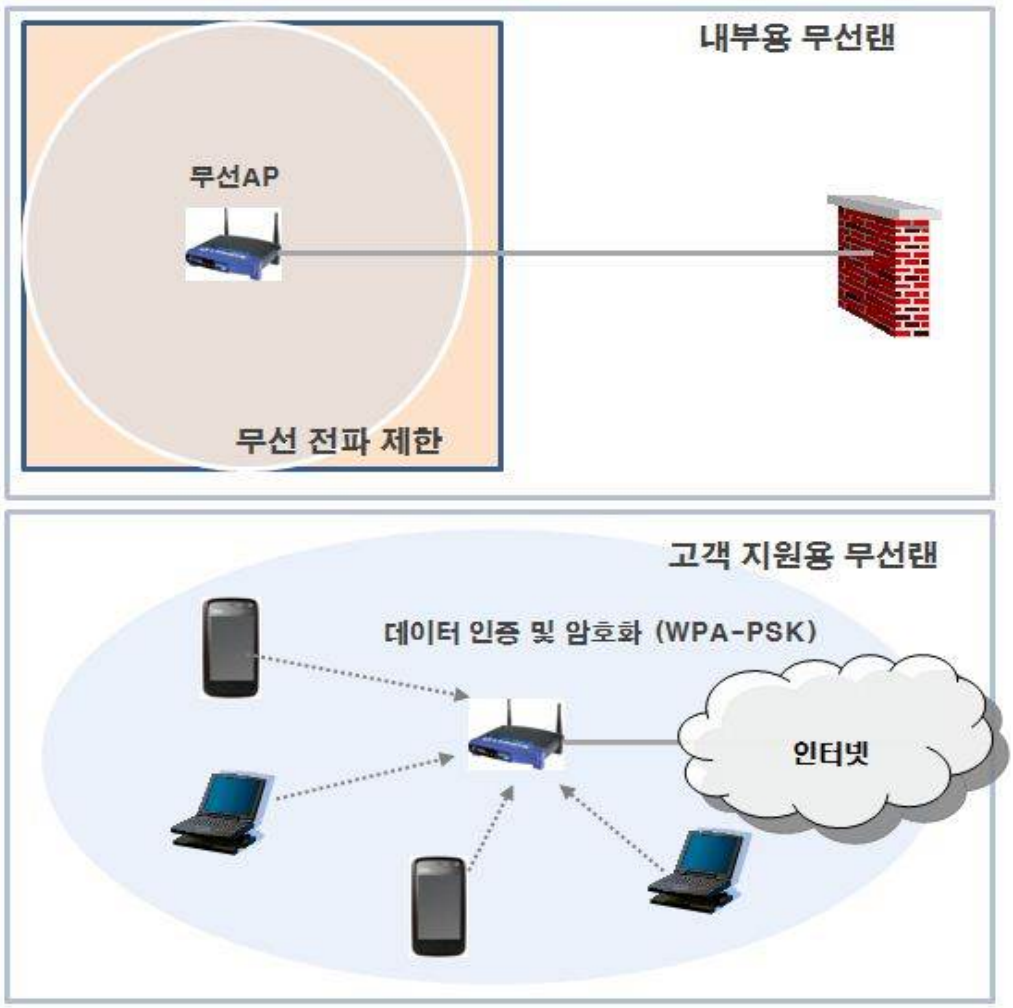


그림 21 고객용 무선랜 구축의 예

제5장

맺 음 말

무선랜은 그 사용 및 운영의 편의성으로 많은 회사에서 도입을 고려하고 있다. 802.11n의 경우 600Mbps이상의 전송속도를 지원하여 유선랜의 상당 부분을 대체할 수 있을 정도이고 무선랜을 초기 설치 후 변경 사항이 많이 발생하지 않아 네트워크 관리자의 입장에서도 관리가 용이해지고 있다. 하지만 무선랜의 특성상 불특정 다수의 접속에 노출되어 있다는 취약점이 존재하므로 초기 구축시 시스템의 보안 수준을 고려하여 구축하고 지속적인 점검을 통해 보안수준을 유지하여야 한다.

적절한 암호화 설정과 사용자 인증을 통해 데이터 유출을 방지하고 불특정 다수에게 무선전파가 전달되지 않도록 보안을 강화하여야 한다. 또한 무선랜 운영시 필요한 고려사항과 유의사항 등을 정책화하여 일관된 기준을 통해 무선랜을 관리하여야 하며 구축된 무선랜을 안정적으로 운영하도록 정기적인 점검 방법 등을 문서화한 관리지침을 잘 활용하여 안전한 무선랜 구축과 운영이 가능하도록 하여야 할 것이다. 또한 교육을 통한 무선랜의 위험성을 인식시켜 기 구축된 보안장비가 무력화되지 않도록 이용자의 보안의식을 향상시키는데 노력해야 할 것이다.

무선랜의 보안 취약성들을 면밀하게 조사하고 안전하게 운영할 수 있다면 무선랜 고유의 편의성을 극대화시키며 유용하고 자유롭게 사용할 수 있을 것이다.

부 록 1. 인증 및 암호화 방식

1. 802.1x /EAP 인증

대칭키 암호는 먼저 통신 당사자들 간에 동일한 비밀키를 소유하고 있어야 하며 이 비밀키를 사용하여 암·복호화를 진행하게 된다. 암호화 방식에 따라 블록 암호와 스트림 암호로 구분되며 DES, AES 및 SEED 모두 블록 암호이며 대표적인 스트림 암호에는 RC4, A5등이 있다.

가. 대칭키 암호알고리즘

- EAP-MD5(Message Digest 5) : MD5 알고리즘을 이용하여 질의/응답 방식의 사용자 인증을 수행하는 방식

- EAP-TLS(Transport Layer Security) : 무선랜 단말기와 서버 간의 인증서 기반의 상호 인증을 제공하며, 보안성은 우수하지만 단말기에 인증서를 설치 및 관리해야 하는 불편함이 존재

- EAP-TTLS(Tunneled TLS) : EAP-TLS의 불편함을 해소하기 위해 무선랜 단말기의 인증서 설치 없이 상호 인증을 제공하는 보안성과 편리성이 우수한 인증방식임

- EAP-LEAP(Lightweight Extensible Authentication Protocol) : Cisco社가 제안한 방식으로 동적으로 생성된 WEP키를 이용하여 전송 데이터를 암호화하며 상호인증을 제공하지만, 보안성이 취약한 것으로 알려짐

- EAP-FAST(Flexible Authentication via Secure Tunneling) : EAP-LEAP를 개선한 것으로 인증서를 사용하는 대신에 인증서버에서 동적 관리할 수 있는 인증터널을 만들어 상호 인증하는 방식

- EAP-PEAP(Protected Extensible Authentication Protocol) : 무선랜 단말기와 서버간 인증터널을 사용하여 상호 인증하는 방식으로서, 서버의 인증서만 설치가 필요한 보안성과 편리성이 우수한 인증방식

- EAP-SRP(Secure Remote Password) : 무선랜 단말기가 인증을 받을때 인증서버와 단말기 간에 ID와 패스워드의 전송 없이 서로 다른 연산값 교환을 통해 인증하는 방식

❍ DES (Data Encryption Standard)

- 64비트 데이터 블록을 56비트 비밀키를 이용하여 암호화하는 대칭키 암호알고리즘
- 56비트라는 짧은 키 길이로 인해 더 이상 안전하지 않다고 판단되어 DES를 3회 반복하는 Triple-DES를 사용하도록 권고

부 록 2. 무선랜 보안 체크리스트

점검 항목	필수 항목	선택 항목
무선랜 사용과 관련된 조직의 보안정책 개발	√	
무선랜 사용자에 대한 보안교육	√	
무선랜카드 및 AP 의 보안 패치 적용	√	
주기적인 보안평가(보안감사) 실시	√	
건물 및 무선랜 장비 사용 장소에 대한 물리적인 접근제어	√	
AP 서비스 범위 결정	√	
보유한 무선랜카드 및 AP의 목록 작성/관리	√	
근접한 AP간의 이종 채널 설정	√	
AP 설치시 외부와 인접한 장소(벽, 창문 등) 회피	√	
인가되지 않은 사용자의 AP에 대한 물리적인 접근 방지	√	
AP 미사용시 전원 차단	√	
인가된 사용자에 의한 AP 리셋 기능 수행	√	
AP 리셋 수행시 설정된 보안 환경으로 복구하는 기능 확보	√	
기본으로 설정된 AP의 SSID 변경	√	
AP의 SSID 브로드캐스트(Broadcast) 기능 차단	√	
AP의 SSID 설정시 부서명, 회사명, 제품명 등의 사용 회피	√	
모든 기본 설정값에 대한 이해 및 변경	√	
128비트 이상의, 가능한 최대 크기의 암호키 사용	√	

기본으로 설정된 암호키를 보다 안전한 값으로 주기적으로 변경	√	
유선 네트워크와 무선 네트워크(AP 또는 Hub to APs) 구간에 침입차단 시스템 설치	√	
무선랜 클라이언트 시스템 안티 바이러스(Anti-Virus) 제품 설치		√
무선랜 클라이언트 시스템에 개인용 침입차단시스템 설치		√
AP 간의 연결을 위해 허브 대신에 레이어 2 스위치 설치		√
교환되는 정보의 중요도를 고려한 적절한 암호 메커니즘 사용		√
주기적으로 소프트웨어 패치 및 업그레이드	√	
모든 AP에 보안강도가 강한 관리 패스워드 사용	√	
모든 패스워드 주기적인 변경	√	
생체인식, 스마트카드, 2중 인증, PKI 등의 사용자 인증 메커니즘 실시		√
고정 IP 사용		√
DHCP 기능 차단		√
AP 관리를 위한 사용자 인증	√	
SNMP의 적절한 설정(쓰기 기능 금지) 및 미사용시 기능 해제	√	
AP 관리시 시리얼 포트 사용		√
무선랜카드 사용자에 대해 RADIUS, Kerberos 등의 사용자 인증 고려		√
무선 통신 구간에 침입탐지시스템(IDS) 설치		√
향상된 보안 기능을 제공하는 802.11 제품 사용		√
보안 기능을 사용전에 보안 기능 숙지	√	
IETF, IEEE 등의 보안 관련 표준화 작업 확인		√

참고 문헌

[1] 무선랜 보안 가이드, 방통위 한국정보보호진흥원 2008.

[2] 무선LAN 의 안전한 사용을 위한 보안대책, NCSC-TR050021.

[3] 무선랜 보안, 한국정보보호진흥원 2002.

[4] WPA 2 Hole 196 Vulnerability - FAQ, AirTight 2010.

[5] 공중 무선랜 망에서 인증 및 키관리 기술동향 ETRI, 2002.8.

[6] 무선랜에서의 보안, 유넷시스템 보안닷컴 2010.

[7] 해외 무선랜 보안 법제도 연구, 한국인터넷진흥원 2010.

[8] 무선랜 활용현황 및 보안 적용 실태, 인터넷정보보호세미나 2010.

[9] ITU-T FMC 표준화 현황 및 국내 대응방안, 고석주 2008.

[10] 무선랜 보안 실태조사 및 분석을 통한 보안강화 방안 연구, 정현철 2006.

[11] "와이파이존 4만2천개", 이데일리
http://www.edaily.co.kr/news/NewsRead.edy?newsid=02223846592974496&DCD=A03101, 2010.5.

[12] 무선랜 WPA 보안 핵심기술, [IT리포트], 한국증권거래소, 2004.10.

[13] 1x 및 무선보안 기본이론, 유넷시스템 2010.

[14] 무선랜 보안 표준 IEEE802.11i, TTA 2010.

[15] WiFi and FMC Service Security, 한국인터넷진흥원 2010.

[16] IEEE Wireless Medium Access Control (MAC) and phtsical layer (PHY) specifications, IEEE Std. 802.11, 1999.

[17] IEEE, Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed physical layer in the 5GHz band, IEEE Std. 802.11z, 1999.

[18] IEEE, Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Higher speed Physical Layer (PHY)

extension in the 2.4 GHz band,IEEE Std. 802.11b, 1999.

[19] IEEE, Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Port-Based Network Access Control, IEEE Std. 802.1x, 2001.

[20] IEEE, Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Specification for Enhanced Security, IEEE Std. 802.11i, 2004.

[21] Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (Draft), NIST, 2007.

[22] The Caffe Latte Attack : How it works and How to block it, Lisa Phifer, 2007.

[23] Cafe Latte with a Free Topping of Cracked WEP - Retrieving WEP Keys From Road-Warriors, Md Sohail Ahmad, Vivek Ramachandran, 2007.

[24] A Comprehensive Review 0f 802.11 Wireless LAN Security and the Cisco wireless security suite, Cisco, 2002.

[25] 비인가 소프트 AP에 대한 무선 보안 방안, AirTight, 2010

[26] 안전한 무선랜 사용자TTA 무선랜 보안안내서, TTA 2005.

[27] 무선 LAN 보안 체크리스트, on the net, 2005.3

[28] '무선LAN'의 보안 취약성 고찰, NCSC, 2005.8.

이 가이드 작성을 위해 다음 분들께서 수고하셨습니다.

2010년 12월

총괄 책임자	금융보안연구원 사이버대응센터	센 터 장	성 재 모
참여 연구원	해킹대응팀	팀 장	이 성 욱
		주임연구원	박 찬 홍
		연 구 원	홍 영 우
외부 전문가	한국기술비젼	대 표 이 사	김 현 승
	UNET	소 장	이 상 준

금융부문 무선랜 보안 가이드

2010년 12월 인쇄

2010년 12월 발행

발행인 : 곽 창 규

발행처 : 금융보안연구원

서울시 영등포구 여의도동 36-1

키움파이낸스 스퀘어 빌딩 15층

Tel: (02) 6919-9114

인쇄처 : 일지사(TEL : 503-6971)

<비 매 품 >