제 25 회 한국정보처리학회 춘계학술발표대회 논문집 제 13 권 제 1 호 (2006. 5)

무선랜 보안 실태 조사 및 분석을 통한 보안 강화 방안 연구

정현철*, 이희조
*고려대학교 컴퓨터 정보통신 대학원
e-mail : change@korea.ac.kr

Study on Security Reinforcement Method by Wireless Security Status Survey and Analysis

Hyun-Chul Jung* , Heejo Lee
* Graduate School of Computer and Information Technology, Korea University

요 약

최근 기업의 무선랜 인프라 도입이 본격화 되고 가정내 유.무선 공유기의 보급으로 인하여 무선랜의 사용이 대중화 되고 있다. 하지만 급속한 대중화 과정에서 무선랜 사용자 및 운영자의 보안의식 부족으로 각종 무선랜 해킹 위협에 노출 되어 있다. 또한 현재의 무선랜 보안 현황이 제대로 파악 되어있지 못해 어떤 부분에 대한 보안이 시급한지에 대한 정보가 부족하였다. 이에 본 고에서는 무선랜 IDS(Intrusion Detection System)를 이용한 무선랜 보안 실태 조사를 실시하여, 실제 여러 지역의 무선랜 보안 현황을 통계치 기반으로 파악하였다. 또한 이를 바탕으로 현재 무선랜 환경에서 가장 중요하고 발생 가능성이 높은 문제점이 무엇인지 제시하고 그 해결을 위한 가이드 라인을 제시하고자 한다.

1. 서론

최근 기업의 업무환경이 정적인 유선에서 동적인 무선으로 변화하고 있으며 이에 따라 무선 네트워크의 구축과 서비스가 활발해지고 있다. 이러한 무선 네트워크 중 무선랜은 유선 네트워크와의 호환성과 무선이 갖는 확장성을 동시에 가지고 있어 많은 기업들이 도입하고 있다. 또한 가정에서도 가정내 유.무선 공유기의 보급으로 인하여 무선랜의 사용이 활성화 되고 있다[1]. 이에 따라 무선랜 보안 제품들도 802.1x 와 WPA 표준기반으로 안전화 되어가고 있다.

하지만 급속한 대중화 과정에서 무선랜 사용자 및 운영자의 보안의식 부족으로 각종 무선랜 해킹 위협에 노출 되어있다. 또한 현재의 무선랜 보안 현황이 제대로 파악 되어있지 못해 어떤 부분에 대한 보안이 시급한지에 대한 정보가 부족하였다. 이에 본 고에서는 무선랜 IDS 를 이용한 무선랜 보안 실태 조사를 실시하여, 실제 여러 지역의 무선랜 보안 현황을 통계치 기반으로 파악하였다. 또한 이를 바탕으로 현재 무선랜 환경에서 가장 중요하고 발생 가능성이 높은 문제점이 무엇인지 제시하고 그 해결을 위한 가이드 라인을 제시하고자 한다

본 논문의 구성은 2 장에서 국내에서 보편으로 사용되고 있는 무선 보안 기술에 대하여 논하고 3 장에서 무선랜 보안 실태 조사와 그 결과에 대하여 논하고 4 장에서 무선랜 보안 실태에 대한 문제점에 대하여 논하고 마지막으로 5 장 결론에서 문제점 해결을 위한 가이드 라인과 향후 과제를 제시한다.

2. 무선랜 보안 기술

무선 보안 기술은 IEEE 이나 Wi-Fi Alliance 에서 제안된 기술들이 널리 사용되고 있다. 이 기술들 중 국내에서 사용자들에게 널리 알려져 있거나, 솔루션으로 제공하고 있는 기술들은 다음과 같다.

1. SSID 숨김

무선 네트워크 ID 인 SSID 를 AP 와 무선랜 Client 간

에 공유하는 인증방식이다. 일반적으로 SSID 를 숨겨주는 기능인 Secure Access 를 사용하는데, 이 경우 지정한 SSID 를 사용해야 무선랜이 가능하도록 하고 있어 보안이 강화되는 측면이 있다. 그러나 SSID 숨김을 하더라도 AP 가 Client 하고 통신을 하고 있는 경우 스니핑 을 통해 SSID 알아 낼 수 있는 취약점을 가지고 있어 최소한의 보안으로 사용되고 있다.

2. MAC filtering

SSID 보다 향상된 보안방법으로 AP 에 접속할 수 있는 Client 의 MAC Address (네트워크 카드의 고유 번호)를 미리 등록해 놓아 기 등록된 MAC 의 접근만을 허용하는 보안기술 이다[2]. 그러나 MAC 자체가 암호화되지 않았을 경우 스니핑을 통해 찾아낼 수 있으며, 이로 인한 MAC Spoofing(MAC Address 도용)이 일어날 가능성이 있다. MAC Filtering 의 또 다른 방법으로는 ACL(Access Control List)을 만들어 지정된 MAC 주소 이외의 모든 주소를 차단시킬 수 있으나, 관리자가 일일이 작업해야 하므로 부담이 커지게 되어 WLAN 시스템의 규모가 큰 경우 RADIUS 서버에 있는 MAC 주소만의 접속을 허용하는 방법을 사용하게 된다. MAC Filtering 은 적용이 쉽고 네트워크 속도 저하가 발생하지 않아 많이 사용되고 있다.

3.WEP 보안

WEP(Wired Equivalent Privacy)은 Wi-Fi 에서 유선과 동일한 프라이버시를 제공하고자 개발된 방법으로, 단말기와 AP 간에 WEP 암호화를 통해 데이터가 이동하는 방식으로 64bit IV(Initialization Vector) 키값이나 128bit 를 사용하며, IV Key 조합의 고갈시 암호 스트림의 재사용이 일어난다. WEP 은 다른 암호 프로토콜에 비해서 구현이 간단하고 사용방법도 편리하여, 무선랜에서 사용자 인증과 데이타 암호화를 위하여 많이 사용되고 있다. 하지만 WEP 는 알고리즘 자체가 IV 의 평문 전송, 키 스트림의 단순성으로 인하여 악의적인 공격자에 의해 WEP 키 값이 노출될 수 있는 취약한 알고리즘 인데다, 단방향 인증 메카니즘으로, Man-in-the-middle 공격이나 Session hijacking 이 가능하고 전송 패킷의 무결성 보장을 위하여 단순한 CRC-32(Cyclic Redundancy Check) 알고리즘을 사용 하여 무선 패킷의 위/변조 공격에 취약하다[3]. 하지만 WEP 는 무선랜 초기부터 제공되어 많은 사용자들이 사용하고 있는 기술이다.

4.IEEE 802.1x 기반 보안

IEEE 802.1x 보안은 인증서버(RADIUS)가 사용자 인증을 수행하여 그 결과에 따라 네트워크 접속을 제어하는 보안 방식이다. 인증 메세지 교환 시에는 이더넷, 토큰링 혹은 무선랜에서 기존의 통신 규약인 EAP RFC 2284 를 사용한다. 데이터 암호화를 위해 WEP 알고리즘 사용이 가능하다. IEEE 802.1x 에서 제공하는 인증은 MAC filtering 이나 WEP 같은 host 별 인증과 달리 사용자 별 인증을 제공할 수 있어 사용자 별 어플리케이션 사용 권한부여 및 인증 등의 기능들을 제공할 수 있다. 또한 IEEE 802.1x 는 현재까지 큰 취약점이 발견되지 않아 안전한 프로토콜로 인정 받고 있다. 국내에서 Enterprise 무선랜을 구축할 경우 가장 많이 쓰이고 있는 무선랜 보안 기술이다. EAP-MD5 를 사용하는 IEEE 802.1X 인증 기능은 무선랜 공중망 서비스를 위한 보안 기술로 주로 사용되고 있다.

5.TKIP 보안

TKIP 은 WEP 알고리즘의 취약점을 보안하기 위해서 개발되었다. TKIP 은 WEP 을 적용할 수 있도록 구성된 무선랜 장비 펌웨어 업그레이드나 소프트웨어 업그레이드를 통해, 사용자 레벨의 보안을 강화하기 위한 방법을 제공하고 있다. TKIP 의 적용은 WEP 이 갖는 취약성을 보완하여 무선랜 보안 기능을 강화하면서 소프트웨어 업그레이드를 통한 보안 기술을 적용할 수 있어, 하드웨어 장비의 추가 설치로 인해 발생할 수 있는 비용을 감소 할 수 있게 한다. 또한 TKIP 는 전송되는 데이터 패킷마다 증가되는 초기벡트인 IV 시퀀스 값을 WEP 키와 함께 해쉬하고, 새로운 WEP 키를 생성하여 각 패킷마다 키 지정이 가능하도록 제공한다. 이러한 것은 새로운 키 생성 함수를 이용함으로써 가능해지는 것이다. 즉, 새로운 키 생성함수에 키 재설정 방식을 적용하여 고정된 WEP 키를 사용할 때 방생하는 키의 외부유출 가능성을 줄여준다[4]. TKIP 기술은 WPA(WiFi-Protected access) 표준으로 새로운 무선랜 장비에서 제공되고 있다.

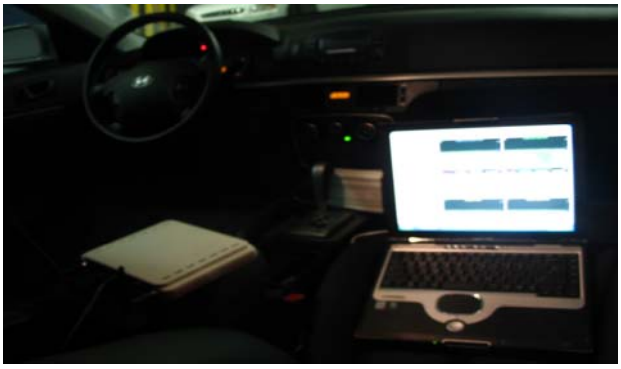
6.VPN 기반 보안

VPN 은 네트워크 기반구조간의 안전한 정보 전송 수단으로 원격 사용자에 대한 접근제어, LAN-to-LAN 연결, 엑스트라넷 등에서 이용되고 있으며, IPSec 을 이용한 기밀성, 데이터 무결성, 리플레이방지, 트래픽 방지 등의 보안 서비스를 제공하고 있다. 무선에서 IPSec 이용은 VPN Device 로부터 AP 를통해 Wireless Client 단말기까지의 터널링으로 이루어진다.[3] IPSec 을 통해 보안 서비스가 이루어질 경우 무선구간뿐만 아니라 유선구간까지 암호화 된다는 장점을 가지고 있다. 또한 기존에 VPN 게이트웨이가 존재하는 경우 사용자에게 Client 에 추가적인 소프웨어만 설치하면 되기 때문에 주로 기존에 VPN 게이트웨이를 보유하고 있는 기업에서 사용되고 있다. 하지만 기업내에 특정 어플리케이션에 대한 인증이나 권한 부여는 VPN 기술로는 해결해 줄 수 없다[5].

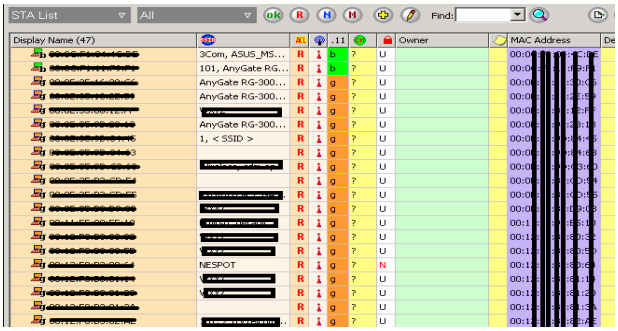
3. 무선랜 보안 시스템 운영 실태 조사

1. 조사 방식

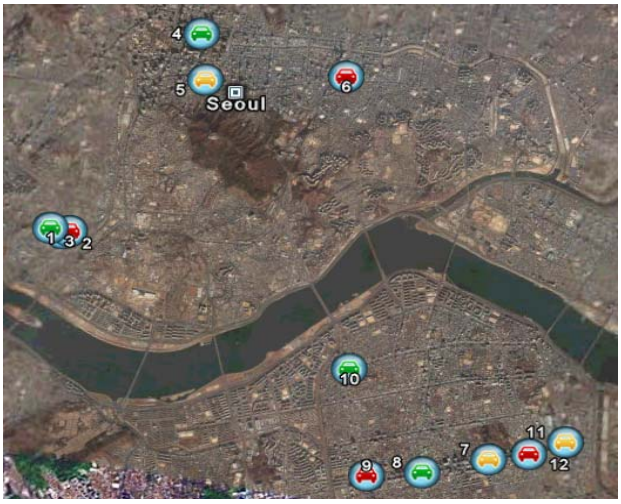
조사방식은 그림 1 과 같이 차량에 무선랜 IDS 시스템(Airmagnet Enterprise 6.1)을 탑재하여 조사를 수행했다. 그림의 왼쪽에 있는 것이 무선랜 시그널을 수집하는 무선랜 센서이고 오른쪽에 있는 노트북에는 센서로부터 수집된 데이터를 전송 받아 분석하는 무선랜 IDS 소프트웨어가 운영되고 있다. 그림 2 는 수집되는 데이터를 보여주는 무선랜 IDS 화면이다. 조사지역 아래의 그림 3 의 경로로 순차적으로 진행했다.



(그림 1) 무선랜 실태조사 장비



(그림 2) 무선 IDS 화면



(그림 3) 무선랜 보안 실태조사 경로

조사 항목은 '무선랜을 사용하고 있는 디바이스 목록', '무선랜 장비중 AP 에서 사용하고 있는 무선랜 보안 기술', '무선랜 해킹 또는 해킹을 위한 사전 행위'에 대하여 조사하였다

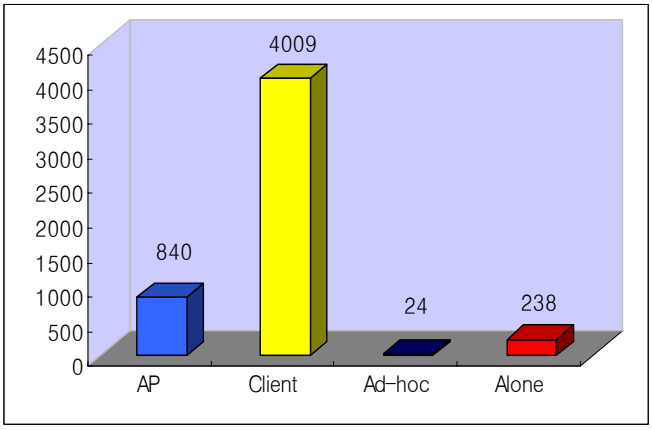
<표 1> 조사 지역별 무선랜을 디바이스 목록

지역	1	2	3	4	5	6
AP	44	60	44	47	40	63
Client	490	361	240	470	57	144
Adhoc	0	0	1	3	0	2
Alone	9	7	15	70	1	7

지역	7	8	9	10	11	12
AP	103	115	84	59	78	103
Client	354	660	423	160	313	337
Adhoc	3	1	1	2	8	3
Alone	11	30	25	12	22	29

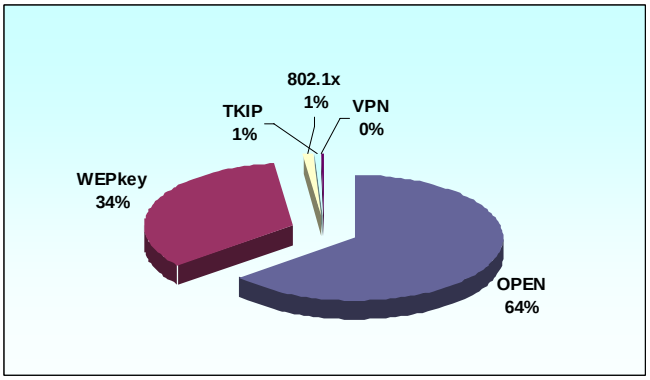
2. 조사 결과

조사된 12 개의 지점별 무선랜 디바이스 목록은 표 1 과 같다. 비 IT 관련 기업 많은 강북 지역 보다는 IT 관련 기업 집중되어 있는 강남의 테헤란로 부근에서 무선랜 사용이 많음을 확인 할 수 있다. 현재 무선랜 사용자들의 무선랜 보안운영 현황 결과를 보면, 그림 4 에서와 같이 12 개 지점에서 수집된 단말기와 AP 의 숫자는 각각 4008 대와 830 대였다.



(그림 4) 종류별 무선랜 디바이스 목록

이들 중 AP 에서 사용되고 있는 보안기술을 조사한 결과는 그림 5 과 같이 아무런 보안기술이 적용되어 있지 않은 Open system 이 전체의 64%이고 WEP 는 34% 있었다. 그 외 802.1x, TKIP, VPN 의 사용은 전체의 2%에 그쳤다.

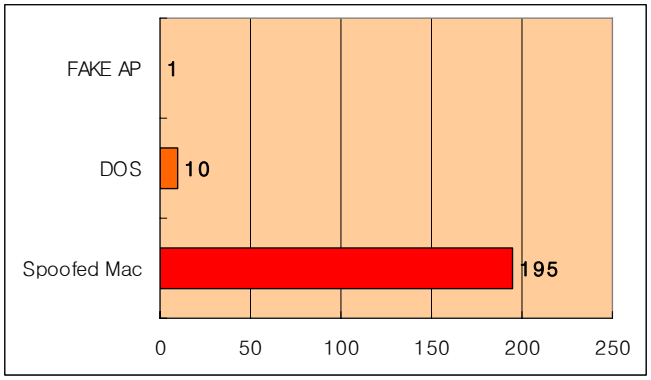


(그림 5) AP 에서 사용하고 있는 무선랜 보안 기술

감지된 무선랜 해킹 및 해킹 사전행위는 표 2 와 같이 206 건이 있었는데 그 중 대부분인 195 건은 Spoofed MAC 이었다. Spoofed MAC 남의 MAC 을 도용해서 MAC filtering 하고 있는 AP 에 불법적으로 접속하거

나, 또는 Man-in-the-middle 공격이나 Session hijacking 위한 사전작업으로 이루어 지는 해킹이다. 그 외에 10 건의 DOS(Denial of Service) 공격도 감지되었는데 모두 한 지역에서 감지된 것으로 보아 한 장비가 MAC 바꿔서 공격하고 있는 것으로 보였고, 가상 AP (FAKE -AP) 사용한 해킹도 감지 되었다.

<표 2> 무선랜 해킹 또는 해킹을 위한 사전 행위



4. 무선랜 보안 운영 실태에 대한 문제점

1.무선랜 보안 알고리즘에 대한 취약성 인식 부족
조사 된 무선랜 시스템 중 64%가 표준기반에 보안 알고리즘을 사용하지 않는 것으로 나타났다. 이는 많은 사용자들이 아직도 MAC 이나 SSID 기반에 기본인증만을 사용하거나 일부는 그 조차도 사용하지 않는다는 것을 말한다. 사용자의 34% 사용하고 있는 WEP 는 앞서 2 장에서 이야기한 바와 같이 IV 의 평문 전송, 키 스트림의 단순성으로 인하여 IV 값을 64 비트 12~13 만개, 128 비트는 100 만 정도를 모우면 WEP Key 추론이 가능하다. 시간적으로도 최신 해킹 툴을 사용하는 경우 64 비트 10 분, 128 비트 40 분 시간이 소요된다. 다시 말해 WEP Key 대단히 취약한 알고리즘임에도 아직도 사용자들은 그것을 인식하지 못하고 있다[6].

2. Mac Filtering 에 대한 과도한 신뢰
2 장에서 말한 바와 같이 Mac filtering 이 많이 사용되고 있지만, 조사 결과에서도 살펴 본 바와 같이 MAC 도형 사례가 많이 발생하고 있다. 또한 현재는 'SMAC' 같은 해킹툴을 굳이 사용하지 않아도 일부 장치는 디바이스 드라이브에서 MAC 수정을 지원하고 있어 MAC 도용이 더욱 손쉬워 졌다. 더 이상 MAC 사용인증 수단으로 사용하는 것은 위험하다.

3. 무선랜을 사용하는 Client 보호 부족.
Standalone Client 란 SSID 는 설정이 되어있어나 현재 찾고 있는 AP 가 없어 접속을 기다리고 있는 Client 를 말한다. 조사 결과에서 Standalone Client 는 전체 Client 의 6% 정도가 확인 되었지만 본고의 조사에서는 SSID 가 판별되지 않는 Client 는 Standalone Client 제외하였기 때문에 실제로는 이보다 훨씬 많은 수의 Standalone Client 이 존재 할 것으로 보인다. Standalone Client 주변에 찾고 있는 AP 가 나타날 경우 사용자에게 아무런 알림 없이 네트워크에 연결 되므로 무선랜 보안에 커다란 취약점이 된다. 사용자가 집이나, 카페에서 무선랜 설정을 하고 사용한 후, 그 설정을 지우지 않고 그대로 회사에서 사용하는 경우 해커는 집이나 카페의 AP 로 가장하여 사용자의 노트북으로 연결 노트북뿐만 아니라 노트북에 유선으로 연결된 회사의 망까지 해킹 가능하게 된다.

5. 결론

최근 기업과 가정의 무선랜 도입이 본격화 되면서 무선랜의 사용이 많아졌고 앞으로도 유비쿼터스 환경에 근거리 통신망의 주력으로 그 사용이 날로 널어 가고 있다. 하지만 앞의 무선랜 보안 실태 조사 결과를 통해 살펴본 바와 같이 현재 무선랜 네트워크는 많은 취약점을 가지고 있다. 그 중에서도 가장 중요한 문제는 '무서랜 보안 알고리즘에 대한 취약성이 인식 부족', 'MAC Filtering 에 대한 과도한 신뢰', '무선랜 사용 Client 에 대한 보호 부족' 있었다.
앞으로 이러한 문제를 해결하기 위해서는 WEP key 같은 무선랜 보안 알고리즘에 대한 취약점을 인식하고 TKIP 같은 대체 알고리즘을 사용 하여야 한다.
또한 MAC filtering 손쉽게 MAC 도용 될 수 있으므로 Radius Server 같은 좀 더 강력한 사용자 인증 시스템이 필요하다. 마지막으로 무선랜을 사용하는 Client 의 보호를 위해서는, 무선랜 사용자들에게 주기적으로 무선랜을 사용하지 않을 때는 무선랜 Disable 할 것을 주지 시켜야 하며, 사용자 관리가 어려운 Enterprise 기업에 경우는 무선랜 IDS 도입을 통한 무선랜 보안이 필수적 이다[7]
현재 나와 있는 무선랜 보안 기술들이 무선랜에 연결된 유선망 자원들을 보호하는데 집중하고 있어 향후 무선랜을 이용하고 있는 Client 에 대한 보호기술에 대한 추가 연구가 필요하다

참고문헌

[1] 신동훈,신동명,고경희 "무선랜 침해사고 예방대책 연구" 2004 년 한국정보과학회 가을 학술발표 논문집 Vol. 31, No2
[2] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specification", IEEE Std 802.11, 1999
[3] J.R. Walker, Unsafe at Any Key Size; An Analysis of the WEP Encapsulation, Tec.Rep. 03628, IEEE802.11 Committee, Mar.2000
[4] 강유성, 오경희, 정병호, "무선랜 보안기술의 진화 동향 및 전망", 전자통신동향 분석 제 18 권 4 호 2003.8
[5] 한국정보보호진흥원 "무선랜 안전운영 가이드" 2004.12
[6] 윤정호 저 "무선 LAN 보안프로토콜" 2005.08
[7] Douglas Toombs 외 19 명 저 "Security 전문가 비밀노트" 2005