무선랜 침해사고 예방대책 연구

신동훈[O], 신동명, 고경희
한국정보보호진흥원
{dhshin[O],dmshin, khko}@kisa.or.kr

Korea Information Security Agency

Dong-Hoon Shin[0], Dong-Myung Shin, Kyoung-Hee Ko

요 약

무선통신기술의 급속한 발달로 유·무선 기술을 이용한 네트워크 구축 및 서비스의 보급이 활발해지고 있다. 이러한 서비스 중에서 무선랜 서비스는 기존 유선 네트워크와의 호환성과 무선이 갖는 확장성으로 인해 많은 곳에서 널리 활용되고 있다. 현재 보급되고 있는 무선랜 제품은 802.1x, WPA 보안 표준을 구현한 제품들이 대부분을 차지하고 있으며, 최근 표준화가 완료된 802.11i 호환 제품들도 많이 보급될 것으로 예상된다. 또한 무선랜 통신의 고속화와 보안기술의 발전에 힘입어 유선구간에서 제공되던 많은 서비스들이 무선환경에서도 비교적 안전하게 서비스될것으로 예상된다. 그러나, 무선랜의 많은 장점에도 불구하고, 많은 기업과 기관에서 무선랜 설치를 망설이는 주요 이유 중의 하나는 무선랜의 보안취약성에 대한 우려 때문인 것으로 분석되고 있다. 물론 무선랜 구축을 위한 추가적인 비용 문제도 있지만, 특히 무선이 유선에 비해 보안이 상대적으로 취약하다는 문제를 제기하고 있다. 이에따라 NIST, DoD 산하 ITRC 및 캐나다의 CSE 등에서는 무선랜 환경에서의 보안취약성 및 모범 사례들을 제시하고 있다. 국내의 경우에는 한국정보보호진흥원에서 무선랜 보안 운영 실태조사를 바탕으로 국내 무선랜 서비스 형태 및 구축방식에 따른 보안대책을 공표하였으며, 일반인을 대상으로한 안전 운영 가이드라인을 마련하고 있다. 본문에서는 국외 무선랜 보안 대책을 소개하고, 무선랜 환경에서의 침해사고를 예방하기 위한 국내 가이드라인의 주요 내용 및 방향을 제시한다.

I. 서 론

무선통신기술의 급속한 발달로 유·무선 기술을 이용한 네트워크 구축 및 서비스의 보급이 활발해지고 있다. 이러한 서비스 중에서 무선랜 서비스는 유선 네트워크와 호환성과 무선이 갖는 확장성 등의 편리함 때문에 많은 곳에서 활용되고 있다. 기존의 무선랜은 802.1x, WPA 표준을 기반으로 하는 보안제품이 현재 많이 적용되고 있으며, 이들 제품은 우수한 업체들의 경쟁적 개발참여로 인해, 안정성을 인정받고 있어 그 수요는 더욱 증가할 것으로 예측된다. 많은 편리성에도 불구하고 많은 기업에서 무선랜 설치를 망설이는 주요 이유 중의 하나는 무선랜의 보안성이 매우 취약하다고 생각하기 때문인 것으로 분석되고 있다. 물론 기존의 유선 네트워크 설비와 비교하여 높은 가격도 주요 이유로 대두되고 있지만, 무선이 유선에 비해 보안이 상대적으로 취약하다는 문제를 제기하고 있다. 반면에, 국내 무선랜 보안 운영 실태조사 결과에서는 무선랜 보안에 대한 사용자의 인식이 낮아 보안취약성에 많이 노출되어 있는 것으로 조사되었다. 따라서 많은 무선랜 사용자가 무선환경에 대한 보안 위협을 막연히 느끼면서도 보안 기능에 대한 이해부족, 불편함 등을 이유로 잘 사용하고 있지 않다는 것을 알 수 있다. 따라서, 국내외적으로 무선랜 보안 취약성에 대한 이해와 함께 무선랜 제품에서 제공하고 있는 보안 기능을 숙지할 수 있도록 보안대책 및 가이드라인을 마련하고 있으며 침해사고 예방을 위한 정부차원의 노력이 진행되고 있다.

II. 무선랜 정보보호 동향

1. NIST의 무선 네트워크 보안대책 연구

미국의 표준 연구 기관인 NIST(National Institute of Standards and Technology)에서는 무선 네트워크 보안을 위해 Draft SP 800-48 : Wireless Network Security[7]를 발간하여 무선랜 보안 대책을 제시하였다. NIST의 무선랜 보안대책에는 무선환경이 갖는 일반적인 특징과 무선 환경의 갖는 기밀성·무결성과 무선 네트워크의 가용성 보장 등의 측면에서 취약성을 분석하였고, 각각에 대한 대응방안을 제시하고 있다. 아래 [표1]은 NIST의 보안대책을 무선랜의 관리적 측면, 운영적 측면, 기술적 측면으로 정리한 것이다.

[표1] NIST의 무선랜 보안대책

구분	보안메커니즘	설 명
관리적	무선랜 보안정책 수립	○ 사용인원, 사용 단말기 파악 ○ 장비설치 권한, 설치장소 제한 ○ 무선랜 통신 정보의 종류 ○ 사용자의 무선랜 사용 절차 ○ 보안사고 발생시 보고, 대처 방법 ○ 보안감사, 평가주기, 범위
운영적	물리적 접근제어	○ 장비에 인가된 사용자만 접근 보장 - 장비 설치장소 사진, 동영상 감시 - 생체인식 장치 설치 등 - 키패드, 암호, 잠금장치 적용 등 ○ AP 서비스 범위 제한
기술적	S/W 보안대책	○ AP 설정시 준수 사항 - 새로운 패스워드 설정 - WEP 암호 긴 값 설정 - MAC접근제어, SSID 변경 사용, DHCP 사용제한 등 ○ S/W 업그레이드 ○ 사용자인증 적용, firewall, WEP 사용
	H/W 보안대책	○ 스마트 카드 사용하여 인증 강도 높임 ○ 무선 VPN, PKI, 생체인식 장치 사용

2. ITRC의 무선랜 공격방법과 보안기술 연구

DoD 산하 ITRC(Information Technology and Operations Center)에서는 무선랜 보안을 위한 연구결과로 802.11 무선랜 환경의 공격 방법들과 보안 메커니즘을 발표하였다.[8] 아래 [표2]는 ITRC에서 제시하는 공격기술과 보안 메커니즘이다.

[표2] ITRC의 무선랜 공격과 방어 기술 연구

	공격방법	공격 메커니즘
공격	Violate the Confidentiality or Privacy of the Session	Traffic analysis
		Passive eavesdropping
		Active eavesdropping with partial known plaintext
		Active eavesdropping with known plaintext.
	Violate the Confidentiality or Integrity of the Data	Man-in-the-middle Attack
	Violate the Integrity of the Network traffic	Unauthorized Access
		Session Hijacking
		Replay Attack.
	방어방법	방어 메커니즘
방어	Integrity Checking	WEP CRC-32 Checksum
		Cryptographic checksum or Message Integrity Codes(MIC)
		Secure hash algorithm SHA-1
	Authentication	IEEE 802.11 Standard or WEP
		Closed System Authentication
		MAC Access List
		Shared RC4 Key Authentication
		802.1x
		WTLS
		Packet Authentication
	Encrypted Tunnel and VPN	OSI network layer and end points
		Encryption algorithm and key size

3. CSE의 무선랜 취약성분석과 정보보호 가이드 연구

캐나다 정부의 통신보안 연구 기관인 CSE (Communications Security Establishment)에서도 무선랜 보안을 위한 취약성 분석 평가와 정보보호 가이드를 위해서" preliminary Vulnerability Assessment of Wire- less LANs"[10]과 "The 802.11 Wireless LAN Vulnerability Assessment(ITSPSR-21)[11]을 발표하였다. CSE에서는 무선랜이 제공하는 보안기술을 설명하고, 무선랜 구축 운영시 발생하는 취약성과 공격방법을 분석하고, 무선랜 환경의 취약성과 공격방법에 대응하기 위하여 무선랜 보안운영의 모범사례와 보안 솔루션을 제시하였다. 아래 [표3]은 CSE 제시하는 무선랜을 위한 모범사례이다.

[표3] 무선랜 사용을 위한 모범사례

모범사례 범주	설 명
Threat and Risk Assessment(TRA)	○ 시스템의 중요성 분석 ○ 공격자의 공격의도, 방법 분석 ○ risk level별 공격 방지, 대응 방법 분석 ○ 공격 대응을 위한 절차 수립
WLAN Policy	○ 무선랜 보안정책을 수립 ○ 기관전체 보안정책과 일치도록 수립
Inventory of Wireless APs and Discovery of Rogue APs	○ 무선랜 AP 명세 기록, 유지 ○ 비인가 AP를 찾기 위한 점검 활동 수행
Monitoring the WLAN	○ 무선랜 traffic 특성 분석.(data/protocol) ○ 비인가자의 traffic 검색.(outsiders) ○ 인가자의 irregular한 traffic 검색

III. 무선랜 정보보호를 위한 대응방안

앞에서는 국내외 연구기관에서 무선랜 보안을 위해 연구하고 있는 연구동향을 무선랜 보안운영의 측면에서 분석하여 보았다. 각 기관에서는 무선랜 보안을 위해 무선랜 보안대책, 체크리스트, 취약성 분석, 공격특성분석, 보안 가이드 라인 등을 제시하여, 무선랜 환경의 안전성, 신뢰성, 기밀성, 무결성 등을 보장하려고 노력하고 있다.

본 논문에서는 우리나라의 무선랜 보안운영 현황을 기반으로, 현재 우리나라에 무선랜 보안운영 현황에 적합한 무선랜 정보보호 개선 방안을 무선랜 취약성에 대한 대응방안과 무선랜 공격기법에 대한 대응방안으로 나누어 제시하였다.

1. 무선랜 보안취약성과 대응방안

무선랜이 갖는 물리적, 기술적, 관리적 취약성을 분류하고 각 취약성에 대응하기 위하 방안을 제시한다. 다음 [표4]는 본 논문에서 제시하는 무선랜 취약성과 대응방안을 정리한 것이다.

[표4] 무선랜 보안취약성과 대응방안

보안취약성		대 응 방 안
AP 불법접근		○ 접근이 용이하지 않은 곳에 설치 ○ AP 보호 케이스 설치
단말기 도난 및 파손		○ 단말기 암호설정, 중요자료백업, 개인정보 등은 저장하지 않음 ○ 단말기 관리 대장 유지
SSID 노출		○ SSID의 숨김모드 적용 ○ SSID를 "NULL" 설정 접속 차단
WEP 관련 취약성	WEP 설정미흡	○ WEP 설정 사용
	WEP 키 노출	○ 최대한 긴 키 사용, 주기적 변경
자동 IP 사용		○ 고정 IP 사용, 무선랜 IP 대역 부여
MAC 주소 노출		○ MAC 주소인증과 다른 인증방법 병행
무선 링크 도/감청		○ WEP, TKIP 등, 무선 패킷 암호화 적용 ○ 무선 VPN 등의 보안 솔루션 적용
유선 네트워크에 설치된 보안 솔루션 우회가능		○ 무선랜 구간, Firewall 설치 운영
비인가 AP 설치	기관내부	○ 보안 정책 명시 ○ 사용자가 비인가 AP 설치 못하게 관리 ○ 주기적인 점검활동
	기관외부	○ 주기적인 점검활동
장비 관리 미흡	장비 운영현황 미파악	○ 무선랜 장비 관리 대장 유지 - 장비목록, 운영현황, 사양, 설정 값 등
	장비의 초기값 사용	○ 모두 새로운 값으로 재설정 ○ 설정 값을 주기적으로 변경
사용자 관리 미흡	보안기능 미설정	○ 사용자 단말기에 보안기능 설정
	보안의식 및 참여의지 부족	○ 무선랜 사용자의 보안의식 고취 - 지도, 교육 및 규제 필요함
AP 전파관리 미흡		○ AP 채널 간섭 점검 ○ AP의 서비스 영역 조절 - AP 출력을 조절

2. 무선랜 공격기법에 대한 대응방안

무선랜은 데이터 전송시 무선 전파를 사용하고 있다. 이로 인해, 무선랜을 통해 전송되는 모든 데이터는 AP 서비스 영역

내부에 있는 다른 사용자에게도 전달된다. 즉, AP 서비스 영역 내부에서, 전송되는 모든 데이터는 도청과 감청의 위협에 노출되어 있는 것이다. 이를 방지하기 위한 노력으로 전송 데이터의 암호화와 사용자 인증을 강화하고는 있으나, 아직까지는 유선 네트워크에 비해 보안상으로 매우 취약하다. 이러한 취약성을 악용하는 침해방법과 이 침해를 막기 위한 노력인 대응방안에 대해서 알아보자. 아래 [표5]은 무선랜 공격기법과 대응방안을 나타내고 있다.

[표5] 무선랜 공격기법과 대응방안 연구

공격 기법		대 응 방 안
Network Discovery	SSID 알아내기	○ SSID의 숨김모드 ○ SSID "NULL" 설정, 접속시도 차단
	IP대역 알아내기	○ 고정 IP 사용 및 무선랜 IP 대역 부여 ○ IP 관리대장 기록유지하여 IP별 사용자 현황 파악
WEP Cracking		○ WEP의 최대한 긴길이 값 설정사용 ○ 키의 주기적 변경, 변경 주기는 짧게 설정 ○ 동적 WEP 사용 ○ WEP을 보완한 WPA의 사용
MAC Address Sniffing		○ 중복 접속되는 MAC Address 탐지 ○ MAC 주소 관리대장 기록유지 ○ MAC 주소별 사용자 현황 파악 ○ EAP 인증, WPA 인증, VPN 등과 연동하여 적용
Man-in-the-middle attack		○ 강력한 상호인증 기술 적용, EAP-TTLS, PEAP이상 ○ WPA 및 802.11i 표준 적용
Session Hijacking		○ 강력한 상호인증 기술 적용, EAP-TTLS, PEAP이상 ○ end-to-end 보안을 위해 VPN 적용
Rogue AP 이용공격		○ 주기적인 무선랜 환경의 점검 실시 - 비인가 AP를 탐지 - 중첩채널 탐지를 통한 전파자원 낭비 방지 ○ AP 관리대장 기록유지, 기관내 AP 현황 파악
DoS Attack		○ AP를 통한 접속 수 제한 설정 ○ MAC 필터링 적용 ○ Firewall, IDS 등 사용, DoS 공격 탐지 및 대응

앞에서도 설명한 바와 같이, 무선은 유선에 비해 보안이 매우 취약한 편이다. 위의 표에서 제시하는 대응방안을 적용하였더라도, 유선에 비해 취약한 무선랜을 완전하게 보호하기에는 미약한 편이다. 다만, 위의 [표4]와 [표5]에서 제시한 대응방안을 적용하면, 현행 무선랜 기술에서 제공하는 보안기능을 최대한 적용한 것이라 볼 수 있겠다.

현재 기존의 무선랜 보안취약성을 극복하고 새로운 공격으로부터 무선네트워크를 안전하게 보호하기 위하여, IEEE 802.11i 표준안에서는 새로운 보안표준과 강화된 보안기술이 채택되었다. 그러나, 아직은 이를 적용한 제품이 거의 없는 실정이다. 향후 802.11i를 적용한 제품의 보급이 늘어나면, 앞에서 살펴본 여러가지 무선랜 보안 취약점을 효과적으로 보완할 수 있을 것으로 예상되며, 무선랜을 이용한 인터넷 쇼핑이나 전자거래, 개인정보 전송등과 같은 중요한 데이터의 전송에서도 사용될 수 있을 것으로 전망된다.

IV. 결 론

무선 통신 기술의 발달로 인해 무선을 이용한 네트워크 서비스가 늘어나고 있는 추세이다. 이중 무선랜은 기존의 유선랜과 호환성이 뛰어나, 사회 많은 분야에서 이용되고 있다. 이러한 무선랜은 일상적인 인터넷 서비스의 사용은 물론이고 업무처리의 효율성을 높여주는 중요한 수단으로 부각되고 있다. 하지만, 앞에서 살펴본 바와 같이, 현재 우리나라의 무선랜 운영 환경은 많은 취약성을 갖고 있다. 이러한 문제점을 보완하기 위해서는 무선랜 서비스를 사용하는 사용자와 무선랜 환경을 구축하여 운영하는 운영자, 그리고 국가기반 네트워크를 관리하는 정부 모두 노력하여야 할 것이다.

특히, 무선랜 운영자는 무선랜 환경이 갖는 물리적 취약성을 점검하여야 한다. 무선랜 단말기의 분실, 도난 파손 방지와 무선랜 장비인 AP에 대한 비인가자의 접근 제한 등을 고려하여야 하고, 무선랜 장비에서 제공하는 보안기능을 활용하여야한다. WEP 설정, MAC 주소 필터링, 무선 전파 출력 조절, 장비 초기값 사용 금지 등의 기본적인 보안 수칙만 지켜도 무선랜을 통한 많은 침해 사고의 가능성을 예방 할 수 있게 될 것이다. 이와 더불어, 사용자 인증의 강화와 무선 데이터의 암호화 설정을 통한 보안성 증대가 더욱 절실할 것이다. 뿐만 아니라, 무선랜 관리자 및 사용자의 보안 정책 수립과 이의 실행 여부 또한 중요하다. 기관에서 수립된 정보보호정책의 원활한 적용과 사용자의 참여의식 고취를 위해 정기적인 정보보호 교육이 필요하고, 이와 더불어 운영자 및 사용자의 자발적인 보안 의식과 참여가 필요하다. 마지막으로, 무선랜을 통한 침해사고 발생시 대응을 하기 위한 대응방법을 준비하고, 이와 관련된 정보교류 및 기술지원 등을 활성화하여 침해사고의 피해를 줄이기 위한 방안을 미리 마련해 두어야 할 것이다.

참 고 문 헌

[1] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specifications", IEEE Std 802.11, 1999.

[2] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specification: High Speed physical layer in the 5GHz band", IEEE Std 802.11a, 1999

[3] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specification: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band", IEEE Std 802.11b, 1999

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

[5] IEEE, "Wireless Medium Access Control (MAC) and physical layer (PHY) specification: Specification for Enhanced Security", IEEE Std 802.11i/D3.0, 2002

[6] 한국정보보호진흥원, "무선랜 보안운영 실태조사 보고서", 2003.11

[7] Tom Karygiannis, Les Owens "NIST Draft SP 800-48 : Wireless Network Security", NIST 2002

[8] Colonel Donald J. Welch, Ph.D. Major Scott D. Lathrop, "A Survey of 802.11a Wireless Security Threats and Security Mechanisms", DoD 2003

[9] Keng Hoe LIM, "Security Guidelines for Wireless LAN Implementation", SANS 2003.

[10] CSE, "ITSG-14 : Preliminary Vulnerability Assessment of Wireless LAN", CSE 2003

[11] CSE, "ITSPSR-21 : 802.11 Wireless LAN Vulnerability Assessment", CSE 2003