# 무선랜 보안 기술 및 운영 현황 분석

김수진* · 서종균* · 한기천* · 정회경**

*㈜유비테크 · **배재대학교 컴퓨터공학과

# Analysis of Tendencies on WLAN Security Technology

Su-Jin Kim* · Jong-Kyun Seo* · Ki-Cheon Han* · Hoe-kyung Jung**

*PaiChai University · **Department of Computer Engineering, PaiChai University

E-mail : giam011@gmail.com, {ice9422, kchan153}@naver.com, hkjung@pcu.ac.kr

## 요 약

오늘날 무선 LAN은 노트북, 스마트폰 등 무선 통신기기의 보급이 일반화됨에 따라 기업의 회의실, 산업용 창고, 인터넷 이용이 가능한 강의실을 비롯하여 심지어 커피숍에 이르기까지 광범위하게 설치되어 있다. 물리적인 침투를 해야만 공격 및 내부정보 접근이 가능한 유선 네트워크에 비해 전파 도달 범위 내의 어디서나 누구나 접속이 가능한 무선 네트워크는 허가되지 않은 사용자에 의한 공격에 상대적으로 취약점을 가지고 있다. 이런 취약점을 방어하기 위해 WIDS/WIPS의 도입이 요구되고 있는 실정이다.

본 논문에서는 무선랜 보안 기술들의 한계점을 알아보고 현재 이루어지고 있는 기술동향을 검토하여 향후 보안문제를 해결할 수 있는 방안을 제시하고자 한다.

## ABSTRACT

Today, as wireless communications devices such as laptops, smart phones are generalized, wireless LAN has been widely installed in the corporate office conference rooms, industrial warehouses, Internet-ready classrooms, and even in a coffee shop. Though a wired network can be accessed and attacked only by the physical penetration, the wireless network which can be accessed anywhere within the reach of anyone has relative vulnerability by unauthorized users' attack. To defend these vulnerabilities, the introduction of WIDS / WIPS is required.

In this paper, we recognize the limitations of WLAN security technology, review the current technology trends and propose the solutions in the future security problems.

키워드

WIDS, WIPS, 침입 탐지, 침입 차단

## Ⅰ. 서 론

정보 통신 기술 발달과 스마트 기기의 보급되어 나이나 성별에 관계없이 무선인터넷 사용이 급격한 증가 추세에 있음을 보여주고 있다. 또한, 무선랜을 통한 인터넷 이용률이 증가하여 무선랜 활용도가 점차 증가하고 있는 것으로 나타나고 있다.

무선랜은 90년 중반부터 유선 랜을 사용하기 힘든 곳을 중심으로 보급되기 시작했고 적용분야가 증가하여 성장세도 빨라졌지만 기업체에서는 보안을 염려해 사용하는 사례가 적었다. 그러나 2009년 스마트 폰 보급 이후 스마트워크, BYOD(Bring Your Own Device) 트렌드가 확산되고 금감원의 무선랜 보안에 관한 지침 등 제도적 이슈가 더해지면서 무선 네트워크 환경 구축이 개인뿐 아니라 기업, 공공부문으로 확대되고 있다.

이러한 상황과는 달리 정부는 '스마트폰 기반 행정서비스' 사업 추진의 일환으로 2000개 이상의 무선 AP를 운영중이나 기술적 보안 대책 미흡으로 무선랜 AP를 통한 내부망 접근을 허용하지 않고 있다. 2013년 3.20 대란 이후 일부 공공기관

은 이동통신사의 공개 AP를 철거 추진한 사례가 있다[1]. 이는 유선 랜과 달리 설치가 쉽고 AP 가청 범위 내에서는 누구나 접근이 가능한 무선랜의 특성으로 인해 많은 취약성을 가지고 있기 때문이다. 이러한 무선랜 보안의 취약점을 극복하고 안전하게 사용하기 위해서는 위험요인을 파악하고 대비할 수 있는 다양한 보안정책과 침입탐지/차단시스템이 필요하다.

본 논문에서는 무선랜의 취약점과 이로 인해 발생할 수 있는 공격 기법들을 분석하고 무선랜 보안의 기술들을 조사하였다. 또한 무선랜 보안 기술들의 한계점을 알아보고 현재 이루어지고 있는 기술동향을 검토하여 향후 보안문제를 해결할 수 있는 방안을 제시하고자 한다.

## Ⅱ. 해외 무선랜 보안 적용 실태

영국은 인터넷 규제를 강화한 '디지털경제법'에 근거해 불법 파일 공유자의 인터넷 계정을 차단하고 공공장소에서의 일정 규모 이상의 인터넷서비스사업자(ISP)에 대해 무선랜 공급을 차단할 의무를 부과하는 등 다양한 정책을 시행중이다[4].

이 법에 따르면, 인터넷서비스사업자가 반복적으로 불법 파일 공유를 시도하는 지식재산권 침해자의 인터넷 속도를 늦추거나 차단할 수 있다. 또 대법원이 저작권 침해 자료를 다수 다루는 웹사이트를 폐쇄할 수 있는 근거 조항도 마련했다.

이밖에도 저작권 소유자가 정기적으로 요구하거나 법이 정한 경우에 ISP들은 관련한 저작권 침해 리스트를 제공해야 하며, 이를 이행하지 않을 경우 법에 대한 불복으로 간주해 누락된 보고당 최대 25만 파운드의 벌금을 부과 하고 있다.

그러나 이 법안은 카페나 레스토랑 또는 개인같이 사설 무선랜 제공자가 제공한 공개 와이파이 네트워크에 누군가 접속해 저작권 침해 행위를 했을 경우 사설 무선랜 제공자의 법적 지위를 어떻게 볼 것이냐에 대한 논란을 낳았고, 이에 따라 영국은 디지털경제법의 주적용 대상인 ISP의 범위를 어디까지로 설정할 지를 구체화하고, 40만 이상의 가입자를 가진 고정형 ISP만을 저작권보호 규정의 규범대상으로 정하고 있다.

미국은 주별로 무선랜 보안 정책을 마련하고 있다. 캘리포니아주는 사업 및 직업법을 통해 무선 접근 포인트 상품의 생산자에게 무선랜 보안을 위한 의무를 부과하고 있다. 소규모 사무실, 재택 사무실, 주거지에서 사용하는 무선AP가 포함된 장치는 소프트웨어에 그 장치의 환경 설정 중 발생할 수 있는 보안 경고를 포함시켜야 하고 소비자에게 그들의 무선 네트워크 연결이 승인되지 않은 사용자가 접근할 수 있음을 알리고 소비자에게 그들의 무선 네트워크 연결을 승인되지 않은 접근으로부터 보호하는 방법을 고지해야 한다.

뉴욕주는 '공공인터넷보호법'을 제정해 무선 인터넷에 대한 보안 조치를 강화해 이를 통해 개인정보를 수집하는 사업자가 무선인터넷을 이용할 경우 최소한의 보안 조치를 의무화했고, 인터넷카페 등 무료 무선인터넷서비스를 제공자에게는 보안 안내 부착을 의무화 하고 있다.

미국 유타주는 인터넷서비스제공자가 유해한 콘텐츠 제공이 우려될 경우 이를 필터링하는 것을 의무화했고 이를 위반할 경우 1만 달러의 벌금을 부과할 수 있도록 하고 있다.

인도는 2008년 9월, 인도 뭄바이에 있는 해군기지 내의 무선랜이 무단 접속에 의해 테러 이메일에 이용된 사건을 계기로 와이파이의 안전한 이용을 위한 규제들을 발표한 후, ISP들에게 4개월의 유예기간을 주고 사용자 정보의 등록제 및 로그인 시스템을 마련하도록 했다.

와이파이 서비스를 제공하는 ISP들이 와이파이의 접근 포인트를 안전하게 해야함을 의무화했고, 모든 접속자들이 안전하게 접속했는지 확인할 수 있도록 와이파이 엔드 포인트에 중앙인증 및 트래킹 시스템을 제공하도록 하고 있다. 이 기록을 1년 이상 보관하며 모든 회원 인증은 정해진 방법을 통해서만 하도록 규제하고 있다.

나이지리아도 상업적 통신 서비스를 위한 와이파이 핫스팟 등록을 의무화하고 보안 관련 규제 가이드라인을 마련했으며, 일본도 '부정액세스행위 금지 등에 관한 법률'을 제정해 권한 없이 컴퓨터 시스템에 고의로 접근하는 것을 금지하고 있다.

## Ⅲ. 국내 무선랜 보안 적용 실태

방송통신위원회와 한국인터넷진흥원이 조사한 결과에 따르면, 국내 무선랜 보안수준이 지속적으로 개선되고 있는 것으로 나타났다. 전국 17개 시·도, 48개 지역에 설치된 무선공유기(AP) 8만 2260대를 대상으로 '무선랜 보안 실태조사'를 실시한 결과, 보안이 적용된 무선랜 비율이 2011년 73.8%에서 2012년 81.6%로 증가됐다고 발표했다.

특히 가정 또는 기업에서 자체적으로 설치·운영 중인 사설 무선공유기의 보안수준이 전년에 비해 크게 향상(50%→62.9%)됐다고 밝혔다. 또한, 무선랜 이용 경험이 있는 만 12세~59세 남녀 1000명을 대상으로 '무선랜 보안인식 설문조사'도 함께 실시한 결과, 무선랜 보안설정 필요성에 대한 인식도 점차 높아지고(78.2%→81.8%) 있는 것으로 나타났다.

그동안 방송통신위원회와 한국인터넷진흥원은 무선랜 이용자들을 대상으로 '안전한 무선랜 이용수칙', '무선랜 보안 웹툰' 등을 제작·배포하는 등 무선랜 보안 홍보활동을 적극적으로 수행해왔다. 이외에도 무선공유기 보안설정 방법을 잘 모르는 이용자들을 위해 스마트폰을 통해 손쉽게 보안을 설정할 수 있도록 지원하는 '무선

랜 지킴이' 앱을 개발해 보급하고 있다.

정부 주도로 무선랜 해킹 및 민감정보 유출 방지 조치의 일환으로 제도/관리적인 수준의 안전한 무선랜 이용 수칙을 발표 했으나, 기술적 조치 부재로 무선랜 해킹 방지에 한계점을 보이고 있다. 무선랜이 유선만큼 안전하지 않으며, 무선해킹에 취약하다는 이유로 관리적 측면에서 정부가 무선랜 보안 지침 및 규제를 강화하여 앞서의 조사와 같이 일부분 효과를 거두고 있으나, 2013년 3.20 대란 이후 일부 공공기관은 이동통신사의 공개 AP를 철거 추진하는 등 기술적 조치의 한계로 실효성을 거두지 못하고 있다.

## Ⅳ. 결 론

무선랜장비의 특성과 무선랜 네트워크 802.11 표준에 정의된 보안 기술의 취약점으로 인해 무선랜 보안위협이 발생할 수 있음을 확인할 수 있었다. 이런 취약점을 방어하기 위해 위험요인을 파악하고 AP에 대한 보안, 인증 및 암호화 적용, 보안 정책의 실행, 보안하고자 하는 영역 내에 어떤 AP와 Station이 있는지 모니터링 해야한다.

이를 통해 불법 AP를 탐지하고 내부 노트북이 외부 AP에 연결돼 내부정보가 유출되는 것을 막을 수 있다. 해커들이 무선 네트워크를 해킹하기 위해 사용하는 해킹툴이나 장비를 탐지하는 위협탐지 장치도 반드시 필요하다. 이를 통해 해킹을 위한 사전행위를 미리 탐지하고 예방할 수 있도록 한다.

무선랜 모니터링과 위협탐지를 위해 제안되고 있는 솔루션이 WIPS(Wireless IPS)이다. WIPS는 AP와 클라이언트간의 상호 인증을 제공하는 기존의 무선랜 인증 서버와는 달리, 보안을 하고자 하는 건물에 무선랜 전용 감지센서를 설치해 건물 주변에 있는 모든 무선랜 기기를 감시하고, 무선랜을 통한 해킹을 차단할 수 있도록 지원한다. 이를 통해 보안 영역 내에서 불법행위를 시도하는 모든 시스템을 무선으로 차단하고 위치를 파악해 관리자가 불법기기를 제거할 수 있도록 지원한다. 전세계적으로 무선랜의 이용이 증가하고 있으며, 보안의 위험성을 인식하고 이에 대한 기술적 대응에 노력하고 있음을 알 수 있다. 안전한 무선랜 이용을 위해서는 정부가 무선랜 보안 지침 및 규제를 강화하고 법제도 개선방안을 마련하는 관리적 차원의 정책도 꾸준히 추진해야 하지만 실효성을 거두기 위해서는 기술적인 지원도 함께 이루어져야 할 것이다.

감사의 글

본 논문은 중소기업청에서 시행한 산학연 공동기술개발사업의 결과입니다.

## 참고문헌

[1] 노병규, 김도우, 김경신, 김효신, “차세대 무선랜 보안 기술동향 및 이슈,” 한국방송통신전파진흥원, Vol1, No3, 2013.2

[2] 백종현, “국내 Wi-Fi 보안 현황 및 안전한 무선랜 이용가이드,” 한국인터넷진흥원, Vol 132, No6, pp.67-72, 2011.2

[3] “알기쉬운 공중 무선랜 보안안내서,” 한국인터넷진흥원, 2011.12

[4] 오병철, “해외 무선랜 보안 법제도 연구,” 한국인터넷진흥원, 2010.7.22