WiFi의 보안문제와 개선방안 연구

김성철* 민대홍**

한국전자통신연구원

A Study on the Security Regulatory Issues in WiFi Network

Sung Chul Kim* Dae Hong MIn**

*ETRI

E-mail : kimsch@etri.re.kr* dhmin@etri.re.kr**

요 약

WiFi는 무선인터넷 접속(Wireless LAN) 방식의 하나로서 이동성, 설치용이성, 유연성 등으로 인하여 널리 사용되고 있다. 더욱이 기존 다양한 디지털 기기들이 WiFi 기반의 application을 탑재하여 각종 온라인 콘텐츠를 이용할 수 있게 하면서 점차 보편적인 인터넷 접속수단으로서 변모하고 있는 상황이다. WiFi의 편리성으로 인하여 기업, 공공기관, 교육기관 등에서 네트워크 구축에 WiFi를 사용하는데 그 추세가 개인부문에서 기업부문으로 확산되고 있다. 하지만 유선인터넷이 케이블이라는 매체를 통해 연결되어 외부와 차폐된데 비해 WiFi는 주파수를 매개로하기 때문에 네트워크 접근이 용이하며 이로인해 보안이 취약해 질 수 있다는 것이다. 이로 인하여 일명 워드라이빙(war driving)이라 불리는 서비스의 무단사용뿐만 아니라 악의를 가진 네트워크 침입이 가능해져 개인정보나 사유재산이 침해 가능성이 높다고 할 수 있다. 이에 본 연구에서는 해외의 WiFi의 보안관련 법제도를 살펴보고 이로부터 국내 WiFi보안을 위한 대안을 제시하고자 한다.

키워드 : 무선랜, Wireless LAN, WiFi, 보안

Ⅰ. 서 론

전화에 이어 초고속인터넷에도 케이블 없이 무선으로 이용할 수 있는 무선랜 기술이 등장하면서 공간의 제약 없이 초고속인터넷을 즐길 수 있게 하는 무선공유기가 가정에 널리 보급되기 시작하였다. 하지만 이러한 무선공유기는 가시적으로 보이지 않는 전파를 이용하고 전파가 도달되는 범위에 있는 타인도 이용할 수 있어 보안측면에서는 취약하지만 국민들의 보안에 대한 관심은 적은 것이 현실이다. 시중에 판매되거나 통신사업자들이 설치해주는 무선공유기에 물론 보안설정 기능이 있으나, 이용자들이 이러한 사실을 모르거나 귀찮다는 이유로 보안설정을 안하는 경우가 많아 무선공유기의 보안위험성을 지적하는 언론보도가 잇따르고 있다.

현재 우리나라에는 약 500만대의 무선공유기가 설치되어 있으며 이중 적어도 74%인 370여만대가 실질적으로 보안설정이 되어 있지 않은 것으로 추정되고 있다. 무보안 무선공유기를 통한 무선랜 접속이 여러 가지 문제점을 가지고 있음에도 불구하고 우리나라는 이를 규제할 수 있는 법적 근거가 없어 사실상 국가의 행정력이 미치지 않는 무풍지대로 남아 있는 실정이다.

이러한 상황이 지속된다면 보안문제, 범죄에의 악용이라는 부작용뿐만 아니라 초고속인터넷 보급률 등 통신인프라 측면에서 세계 최고의 IT강국인 한국의 이미지가 무보안 무선공유기 범람으로 한순간에 추락할 우려도 있다. 따라서 무보안 무선공유기의 범람을 방지할 수 있는 방안을 모색하는 것은 시급한 과제라고 할 수 있다.

이에 본고에서는 국내 WiFi 보안현황을 살펴보고, 해외의 사례를 살펴 국내 WiFi의 보안을 위한 방안을 살펴보고자 한다.

Ⅱ. 국내외 WiFi AP의 보안상황

가. 국내 무선공유기 사용 및 보안 현황

현재 국내에는 약 500만대의 WiFi AP가 보급되어 있는 것으로 추산되는데, 인터넷전화 사업자들이 마케팅용으로 무선공유기를 이용자들에게 제공된 것이 185만대, 일반 소비자들이 마트, 전자상가 등에서 무선공유기를 구매하여 설치한 사설 WiFi AP는 약 315만대로 추산된다.

Nespot 등 통신사업자가 제공하는 WiFi 무선

랜 서비스는 가입자 인증이 없을 경우 네트워크 접속이 불가능했으나, VoIP 사업자들이 마케팅용으로 제공하는 AP나 일반인들이 직접 설치하는 AP는 대부분 무인증으로 쉽게 접근 가능해 500만대의 WiFi AP 중 적어도 74%가 무보안일 것으로 추정된다.

인터넷전화 사업자들이 제공하는 무선공유기의 경우 사업자별로 모든 공유기에 동일한 PW를 초기값으로 설정하여 누구나 접속이 가능하므로 사실상 보안이 설정되지 않은 무보안 상태임[1]이며, 일반 소비자들이 설치하는 무선공유기의 경우 모든 무선공유기에 PW 설정기능이 있으나 대부분 이용자들은 편의상 보안설정을 하지 않은 채로 무선공유기를 사용하고 있다.

<국내 WiFi AP 보급 현황>

네스팟	Mega-AP	MyLG070	사설AP	계
20만대	5만대	160만대	315만대	500만대
서버 보안	동일PW	동일PW	65%가 무보안	74%가 무보안

출처 : 방송통신위원회

우리나라의 경우 해외 주요국들에 비해 개인들의 보안의식이 높지가 않아서 무보안 WiFi AP가 많은 편으로 판단된다. 영국의 가격비교 사이트인 moneysupermarket.com이 '08.8월 조사한 결과에 따르면, 영국 가정의 16%만이 보안을 설정하지 않은 무보안 상태인 것으로 나타났으며, 일본은 개인들의 보안의식이 높아 대부분 개인이용자들이 AP를 설치할 때 보안설정을 하고 있는 것으로 나타났다. 한편 2006년 고려대학교 컴퓨터정보통신대학원이 무선랜 운영실태를 조사하기 위해 서울 시내에 설치된 약 5천개의 무선 AP를 조사한 결과, 보안을 전혀 설정하지 않은 오픈시스템 상태인 것이 65%에 달하며 간단한 툴로 해킹이 가능한 WEP방식의 보안을 설정한 곳은 35%였으며, 높은 보안규격인 802.1x EAP 인증이나 VPN을 사용하는 것은 2%에 불과한 것으로 나타나고 있어 WiFi AP의 보안이 취약한 것으로 나타나고 있다.

나. 해외의 무선공유기 무단접속에 대한 법제현황

우리나라의 경우 무보안 무선공유기 접속을 규율할 수 있는 법제도가 존재하지 않으나 해외에서는 이를 규제하기 위한 법제도가 정비되어 있다.

미국의 경우, 여러 주에서 무인증 WiFi 접속과 관련하여 이를 규제하는 법률이 있는데, 대표적인 법률은 다음과 같다.

① 플로리다 州

플로리다 주 헌법 815.06절은 승인받지 않고 타인의 컴퓨터, 컴퓨터 시스템 또는 컴퓨터 네트워크에 고의로 접속하거나 접속 시도 자체만으로도 불법으로 금지하고 있다. 이와 관련하여 다음과 같은 행위를 금지하고 있다.

- 승인 받은자가 컴퓨터 시스템을 이용하는데 장애를 야기하는 행위
- 컴퓨터, 컴퓨터 시스템, 컴퓨터 네트워크를 파괴하거나 손상 및 장애를 주는 행위
- 컴퓨터, 컴퓨터 시스템, 컴퓨터 네트워크에 감염된 컴퓨터 시스템의 연결

② 미시건 州

미시건 주는 승인받은 컴퓨터, 컴퓨터시스템, 컴퓨터 네트워크에 대한 접속을 방해하는 것을 금지하고 있으며, 이와 관련하여 다음과 같은 행위를 금지하고 있다.

- 컴퓨터, 컴퓨터 시스템, 컴퓨터 네트워크, 컴퓨터 프로그램의 손상, 삭제, 지적재산물의 파괴를 위한 접속이나 접속시도
- 컴퓨터, 컴퓨터 시스템, 컴퓨터 네트워크, 컴퓨터 프로그램의 손상, 삭제, 지적재산물의 파괴 혹은 이들 서비스를 이용할 목적으로 알지 못하거나 원하지 않는 프로그램의 설치

③ 일리노이 州

미국의 일리노이주에서는 Public Act 92-0728 General Assembly에서 통신서비스의 무단이용 및 이러한 행위를 하는 자에게 협력하는 것을 금하고 있다. 이와 관련하여 다음과 같은 행위를 금하고 있다.

- 특정인이 통신서비스 제공자의 승인을 받지 않거나 요금을 지불하지 않고 무단으로 서비스를 이용하거나 획득하는 행위
- 통신서비스 제공자를 편취할 의도로 서비스를 이용하거나, 이를 도와주는 행위
- i) 통신서비스를 대가지불 없이 사용하거나, ii)승인없이 서비스를 편취하기 위하여 불법적인 기기의 사용, 소유, 제작, 판매, 운반, 임대, 광고하는 행위

영국의 대표적인 WiFi AP 무단접속 규제법안으로 컴퓨터오용금지법(CMA ; Computer Misuse Act)이 있는데, CMA는 컴퓨터 시스템의 부정사용을 처벌하기 위한 사이버범죄 법률 중 하나로 컴퓨터 자료에 대한 무단 접근이나 변경을 막고 유죄로 판결되는 무단접근과 무단변경의 경우를 명시하고 있다. 동법 제1절과 제2절에서는 타인의 컴퓨터 자료에 접근하는 것과 승인받지 않고 접근하는 것을 금지하고 있으며 2006년 치안법(Police and Justice Act)에 의해 개정되었는데, 이 법 35절에서는 불법적인 접속에 대한 처벌을 강

1) AP PW를 변경하는 기능을 갖고 있으나 대부분 가입자들은 변경하지 않고 초기 PW를 그대로 사용

화하였다.

일본은 부정액세스 행위의 금지 등에 관한 법률을 1999년 8월 통산성・우정성(총무성)・경찰청이 공동 입안한 법률로 제정하여 정보시스템의 취약성을 악용하는 부정 액세스 행위[2]를 기초로 이루어지는 범죄에 대한 금지 및 처벌 규정을 명시하고 있다. 부정액세스 행위의 금지 등에 관한 법률은 부정액세스행위를 금지하고, 그 위반에 대하여 벌칙을 두고, 타인의 식별부호를 무단으로 제공하는 행위를 금지하고, 그 위반에 대하여도 벌칙을 두는 것을 주요내용으로 하고 있다.

러시아의 경우에는 WiFi를 사용하기 위해 정부의 승인을 받도록 하는 강력한 규제를 단행하도 있는데, 러시아에서는 모든 WiFi를 지원하는 기기를 정부에 등록해야 하며, 기기를 사용하기 위해서는 정부의 승인이 필요하다. PDA, 랩탑과 같은 일반적인 기기는 승인을 받기 위해서는 약 10일간의 기간이 소요되며, 정부에 징발된 기기는 승인없이 이용이 가능하도록 하고 있다. 특히, 가정에서 WiFi 라우터나 AP를 사용하기 위해서는 신청서를 제출하고 정부로부터 면허(license)를 받아야 하며, 모스크바나 상트페테스부르크 같은 지역에서는 연방경찰의 특별허가를 받아야 이용이 가능하도록 하고 있다.

III . 무보안 WiFi AP 확산의 문제점

가. 무선랜의 특성에 따른 보안의 취약성

무선랜은 유선랜에 비해 구축이 편리하지만 보안에 취약한 구조로 알려져 있다. 무선랜은 네트워크 케이블 대신 전파를 이용해 네트워크를 구축하므로 구축시간, 경비 등이 대폭 절감되는 장점이 있으나 주파수를 이용하는 open system이기 때문에 보안에 크게 취약한 구조이다. 특히, 기업들은 다양한 보안 솔루션을 통해 무선랜 보안환경을 구축하고 있으나 일반인들이 설치하는 AP는 무보안상태로 있어 보안위험에 그대로 노출 되어 있다. 무보안 무선공유기는 전파수신 범위에서 누구나 무단 접속이 가능하여 스팸메일, 바이러스, 스파이웨어 등에 쉽게 노출된다. 더욱이, AP를 이용하여 다른 네트워크에 접속하여 해킹하는 경우 추적이 어렵기 때문에 또 다른 범죄의 가능성도 제기되고 있는 실정이다.

나. 서비스 가용성의 우려

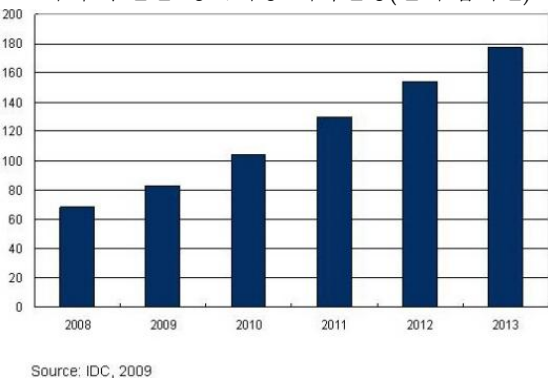
인터넷에 떠도는 간단한 서비스 거부(DoS: Denial of Service) 공격 툴을 내려 받고, 노트북 PC와 무선랜 카드만 있으면 빌딩 전체의 무선랜 인프라를 공격해 서비스를 마비시킬 수 있다. 특히 무보안 무선공유기를 통한 침입은 나중에 추적을 하더라도 접속한 컴퓨터가 아닌 무선공유기 IP만 남기 때문에 추적이 불가능하다.

다. 무선랜이 접목된 유비쿼터스 환경의 위험성 증대

무선랜은 기술발전으로 전송속도에서 갖는 약점을 보완하고 이용 및 설치의 편리성으로 인해 국내의 무선랜의 이용이 점차 증가하는 추세로서, 무선랜 기반의 서비스를 통해 네트워크의 구조에 변화를 예고하고 있다.

유비쿼터스 환경에서 각종 기기의 작동 및 제어에 무선랜 방식이 근거리 통신수단으로 사용될 것으로 예상되면서 무선랜은 유선네트워크를 대체할 새로운 국가신경망으로서 역할을 담당하고 있다. 물류업체 화물의 입출고, 무선POS(Point of Sales)로 처리하는 백화점이나 소중한 환자의 생명과 직결된 병원의 시스템, 일반 기업의 네트워크에의 무선랜 방식의 도입이 대표적 사례라 할 수 있다. 장차 유비쿼터스 환경이 구축되어 가면서 교통통제, 보안, 소방, 의료 등 다양한 부문의 기기를 작동 및 제어하는데 필요한 근거리 통신수단으로 유선방식 뿐만 아니라 Wi-Fi에 기반한 무선랜 방식도 함께 사용될 것으로 예상됨에 따라 보안의 중요성은 점차 증대되고 있다.

<국내 무선랜 장비시장 예측전망(단위:십억원)>



Source: IDC, 2009

라. 네트워크 기반의 홈 네트워크의 위험요인

생활가전과 정보시스템이 유무선 통합 네트워크로 운영되는 홈네트워크는 IP망을 통해 가전의 원격제어가 가능해지고 있다. 가정내 홈네트워크 환경이 점차 무선・ IP환경으로 발전해 가면서 WiFi가 홈네트워크 기기간 연결 및 제어 수단으로 사용될 것으로 예상된다. 허술한 WiFi 보안으로 인한 홈네트워크의 외부침입은 가전기기의 오작동 등으로 인명피해나 재산피해를 야기할 수 있는 만큼 실질적인 안정대책의 인환으로 WiFi의 보안강화 대책이 필요하다.

2) 부정액세스행위 : 액세스 제어기능을 가진 특정 정보시스템 등에 전기통신회선을 통하여 타인의 식별부호 등을 입력하여 작동시키거나, 해당 액세스 제어기능에 의하여 제한되어 있는 특정 기능은 이용할 수 있는 상태로 만드는 행위

Ⅳ. 결론 및 시사점

현재 국내에 보급되어 있는 WiFi AP의 가장 큰 문제점은 AP의 보안설정이 제대로 이루어지지 않고 있다는 점이다. 시장에서 개인이 구입하여 사용하는 무선 AP의 경우, 상품 출시 시 사용자의 설치를 용이하게 한다는 명분으로 암호장치가 해제되어 있는 것이 대부분이다. 출시되는 AP 장치 거의 대부분은 인터넷 보안설정이 해제된 상태로 출고되어, 구매자가 사후에 별도로 보안설정을 해야만 보안기능이 작동하도록 되어 있다. 보안기능이 설정되지 않고 AP가 출고됨에 따라 네트워크 보안에 대한 지식이 없는 사용자는 보안설정을 하지 않는 상태로 이용할 가능성이 높다 할 수 있다. 또한 SoIP용으로 제공되는 AP는 통신사별로 동일 PW 부여되어 있어 무단접속 사용에 노출되어 있는 실정이다. 이러한 문제를 해결하기 위해서 제조업체에 대한 AP 보안설정 강제화가 하나의 대안이 될 수 있을 것이다. 이는 무선 AP제조업자로 하여금 제품 출고 시 현행과 같은 보안 無설정이 아니라, 무작위로 이루어진 보안키를 설정하여 출고토록 강제화하는 방안이다. 예를 들어 AP 제조시에 난수발생 소프트웨어를 탑재하여 구동시마다 16진수 방식의 난수를 발생하여 새로운 암호화 설정을 하도록 암호설정 과정을 자동화는 방식을 도입하는 것이다. 이를 위해 'AP별로 고유PW 설정을 의무화' 또는 'AP에 보안위험 및 PW설정을 권장하는 문구를 표기' 하도록 전파법 제45조(기술기준) 관련 기술기준 고시(무선설비규칙 제98조) 개정할 필요가 있다.

법제도적인 측면에서는 통신서비스의 불법사용을 방지하기 위한 노력이 함께 강구되어야 할 것이다. 현행 법규상에서는 통신서비스의 합법적인 이용과 불법적인 이용의 구분이 제대로 되어 있지 않다. 통신서비스 합법적인 사용과 불법적인 사용을 규정하고 그 범위를 명확히 함으로써 통신서비스의 올바른 사용을 유도할 필요가 있다. 이를 위해서 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제48조(정보통신망 침해행위 등의 금지)에 타인의 통신서비스 무단접속 금지조항 신설이 필요하다.

강제적인 법제도적인 절차 이외에도 비인증 WiFi AP에 대한 보안 및 통신품질 등 예상피해를 홍보하여 이용자 스스로가 WiFi에 대한 보안을 강화토록 함과 동시에 무단 접속의 위험성을 자각하여 무단접속 사례가 발생하지 않도록 하는 대책 또한 필요하다 할 것이다.

참고문헌

[1] The 2008 Florida Statutes CHAPTER 815, Florida State

[2] Michigan Act Section 752.794 FRAUDULENT ACCESS TO COMPUTERS, COMPUTER SYSTEMS, AND COMPUTER NETWORKS, Michigan State

[3] Computer Misuse Act, UK parliament

[4] Police and Justice Act 2006, UK Parliament

[5] 액세스 행위의 금지 등에 관한 법률, 일본 총무성

[6] 무선인터넷 보안가이드, 방송통신위원회, 2008

[7] 무선랜 보안 실태 조사 및 분석을 통한 보안 강화 방안 연구, 한국정보처리학회 추계학술대회, 2006. 5