IoT 환경에서 사용자의 보안수용성 향상을 위한 무선공유기 활용도 조사

홍승완*, 이효직**, 나원철***, 장항배****
*중앙대학교 산업융합보안학과
**, ***중앙대학교 융합보안학과
****중앙대학교 산업보안학과
e-mail: {sw25sw25*, shjlee7**, onechulnastop***}@gmail.com,
hbchang@cau.ac.kr****

A Study on Use of Wireless Router For Security Acceptance Enhancement In IoT Environment

Seungwan Hong*, Hyojik Lee**, Onechul Na***, Hangbae Chang****
*Department of Industrial Convergence Security, Chung-Ang University
**, ***Department of Convergence Security, Chung-Ang University
****Department of Industrial Security, Chung-Ang University

요 약

IoT 환경에서 무선랜의 사용률은 매년 증가하고 있고 그에 따른 무선공유기의 보안은 매우 중요함에도 불구하고 다수의 사용자들은 보안수용성이 낮은 것으로 조사되어 이에 대한 연구를 진행 하였다. 본 논문은 한국 사용자들의 무선공유기 활용도를 조사하고, 보안수용성과의 연관성을 분석하여 보안수용성의 향상을 위한 방안을 제시하는데 목적이 있다. 본 논문의 조사에 따르면 대부분의 사용자들은 무선공유기에 대한 보안수용성이 부족하며 간단한 보안방법 조차 실행하지 않았다. 이를 바탕으로 사용자의 보안수용성은 현재 매우 낮다는 것을 알 수 있으며 보안수용성의 향상을 위한 가이드라인을 제시하였다. 본 논문은 사용자들에게 보안의식을 심어주고 보안에 쉽게 접근하게 할 수 있는 보안수용성 향상의 기반으로 유용하게 사용 할 수 있을 것으로 기대된다.

1. 서론

최근 한 명의 사용자가 다양한 전자기기를 사용하기 때문에 가정이나 회사, 학교 등 많은 장소에서 수많은 무선공유기들이 사용되고 있다. 기업들도 자신들의 서비스를 위하여 카페나 지하철 등 무선공유기를 이용한 무선랜이 가능하게 하였고 이제는 무선랜을 찾아 인터넷에 연결하는 것이 어렵지 않게 되었다. 또한 스마트폰의 사용 뿐 아니라 IoT(Internet of Things)의 발전으로 인하여 무선랜은 이제 빼놓을 수 없는 생활의 중요한 요소가 되었다.

무선공유기의 보안은 여러 가지가 있지만 흔히 사용자들이 암호를 걸고 보안을 할 경우 다음과 같은 방법이 사용된다. WEP(Wired Equivalent Privacy), WPA(Wi-Fi Protected Access), WPA2(Wi-Fi Protected Access2)가 사용되지만 WEP방식 같은 경우는 컴퓨터의 성능이 증가함에 따라 해킹 하는데 몇 분 걸리지도 않을뿐더러 해킹 툴도 쉽게 구할 수 있는 편이기 때문에 널리 사용되지는 않는다. 이렇게 다양한 방법들이 있지만 막상 사용자들은 이것이 어떤 역할을 하는지도 모르고 있는 경우가 많기 때문에 보안 없이 공개적으로 사용하는 경우도 많이 있다. 이러한 행동들은 보안의 취약점을 발생시켜 본인뿐만 아니라 남에게도 피해를 줄 수 있다. 무선공유기는 우리나라 뿐만이 아니라 외국에서도 많은 보안문제를 발생 시켰고, 실제로 보안이 취약한 가정용 공유기를 이용하여 DDos공격을 일으키는 사례도 보고된 바가 있다. 또한 보안이 허술한 공유기에 침투하여 접속 DNS를 위조한 후 해당 공유기를 사용하는 기기들이 인터넷 접속 시 변조된 사이트로 유도하여 개인정보를 해킹하는 방법도 최근 늘어나고 있는 추세이다.

IoT 환경에서의 무선랜은 우리의 생활에서 빼놓을 수 없는 밑바탕이 되었다. IoT 환경에서는 무선공유기가 중심이 되어 데이터를 주고받게 될 것이기 때문에 나에 대한 모든 정보의 허브라고 할 수 있다. 하지만 사용자들의 무선공유기 보안에 대한 인식이 바뀌지 않는다면 무선공유기는 해커들의 좋은 먹잇감이 될 것이다. 해킹을 통하여 사용자의 정보를 빼앗아 가는 것은 물론 본인도 모르는 사이에 사이버 공격에 가담하거나 피해자가 될 수도 있다. 따라서 본 논문에서는 IoT 환경에서 사용자의 보안수용성 향상을 위한 무선공유기의 활용도 조사를 하고자 한다.

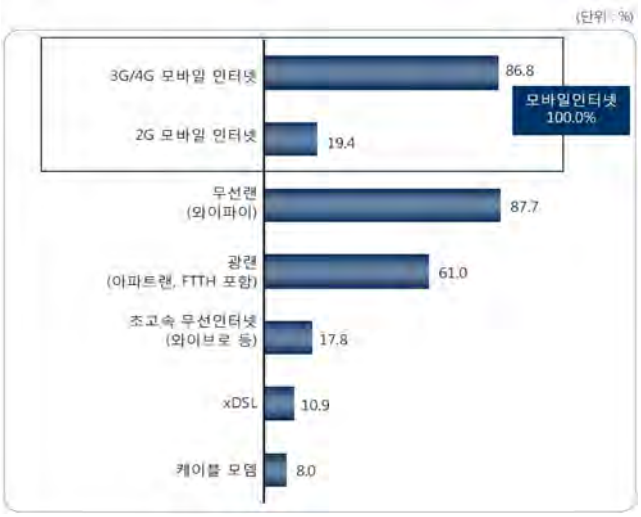
2. 무선공유기의 보안 및 활용 실태 조사

IoT 환경에서 한국의 인터넷 접속률은 한국인터넷진흥

* 제 1저자

**** 교신저자

원의 “인터넷이용실태조사”에 제시되어 있으며, 사용자들의 접속률은 매년 증가하는 추세를 보이고 있다. 또한 (그림1)과 같이 사용자들이 인터넷에 접속하는 방법으로는 무선랜를 이용한 방법이 87.7%가 될 정도로 많이 사용한다는 것을 알 수 있다.



(그림 1) Wi-Fi를 이용한 인터넷 접속률

높은 이용률을 보이는 무선랜의 인프라를 구축하기 위해서는 무선공유기를 사용하게 되는데 IoT 환경에서는 무선공유기가 모든 사물들의 허브 역할이 될 것이기 때문에 무선공유기의 보안은 상당히 중요하다고 할 수 있다. 무선공유기의 보안기술은 여러 가지가 있지만 우리가 흔히 사용하는 보안기술은 WEP, WPA, WPA2가 있고 각각의 보안기술은 다음 <표 1>의 방법이 사용된다.

<표 1> 무선공유기 보안기술

구분	WEP	WPA	WPA2
인증	사전 공유된 비밀키 (64비트, 128비트)	사전 공유된 비밀키 또는 별도의 인증서버	사전 공유된 비밀키 또는 별도의 인증서버
암호방법	고정 암호키 RC4 알고리즘	암호키 동적 변경(TKIP) RC4 알고리즘	암호키 동적 변경(AES) 등 강력한 암호 알고리즘
보안성	가장 취약 널리 사용 되지 않음	WEP 방식 보다 안전 불완전한 알고리즘	가장 강력한 보안기능 제공

방송통신위원회의 “정보보호 실태조사”를 보면 사용자들의 정보보호 인식 수준은 매우 높다는 것을 알 수 있지만 무선공유기 예방조치를 본다면 보안수용성은 매우 낮다는 것을 알 수 있다. 이 결과는 사람들이 보안의 중요성은 인식하지만 실제로 행동으로는 옮기지 않는다는 것을 의미한다. 이러한 현상은 보안에 커다란 구멍을 만들게 되며 본인뿐만 아닌 남에게도 큰 위협이 된다.

무선공유기의 활용 실태는 <표 2>의 항목으로 조사하였다. ‘무선공유기의 보안유무’는 사용자들이 무선공유기를 사용 할 때 암호를 걸어 사용하는지 조사하고 만약 암호를 사용하지 않는다면 그 이유는 무엇인지를 조사한다. ‘무선공유기 보안기술’항목은 위의 질문에서 암호를 사용할 시 보안기술은 WEP, WPA, WPA2중 어느 것을 사용하는가에 대한 질문이고 ‘무선공유기 암호패턴’은 암호의 패턴이 연속성을 가지거나 같은 문자를 반복하는 단순 패턴인지 다양한 문자들을 섞어 유추하기 어려운 복잡한 패턴인지를 말하며, ‘보안수용성’항목은 사용자들이 보안을 어떻게 받아들이며 해야 할 것으로 생각하는지에 대한 것을 말한다. ‘제공자가 불명확한 무선랜’은 평상시 무선랜이 필요할 때 제공자가 불명확한 무선랜이 검색 되더라도 그것을 사용하거나 비밀번호가 걸려있다면 단순패턴의 비밀번호라도 입력해서 사용을 해보려고 하는지에 관한 것을 말한다.

<표 2> 무선공유기 활용 실태 조사 항목

조사항목	내 용
무선공유기 보안유무	무선공유기 암호 사용 여부
무선공유기 보안기술	WEP, WPA, WPA2
무선공유기 암호패턴	단순, 중간, 복잡
보안수용성	보안에 대한 수용성
제공자가 불명확한 무선랜	제공자가 불명확한 무선랜의 사용 여부

‘무선공유기 보안유무’은 사용자들 중 56%만이 암호를 사용한다고 답하였고 그 중 ‘무선공유기 보안기술’의 대한 응답으로는 WEP 32%, WPA 20%, WPA2 38%가 나왔으며 모르겠다는 응답도 10%나 나왔다. ‘무선공유기 암호패턴’은 단순패턴 40%, 중간패턴 34%, 복잡패턴 26%로 응답하였다. 무선공유기에 암호를 사용하는 사용자중 WPA, WPA2의 보안기술을 사용하며 암호를 중간패턴 이상으로 사용하는 사용자만을 안전한 보안으로 가정한다면 보안을 제대로 사용하는 사용자는 약 20% 수준이라고 생각 할 수 있으며, 나머지 사용자들은 무선공유기의 보안이 취약하다고 볼 수 있다. 또한 ‘보안수용성’을 조사해본 결과 위의 항목에서 안전하게 무선공유기를 사용하는 사용자들이 보안을 당연하게 받아들이며 보안을 매우 중요하게 생각하여 관심을 가지고 보안설정을 적용한다는 것을 알 수 있었다. 하지만 상대적으로 보안이 취약한 사용자들은 보안이 막연하게 중요하다는 것은 인식하고 있지만 막상 어떻게 해야 하는지 잘 모르거나 귀찮아서 보안을 하지 않는 경우도 많았다. 마지막으로 ‘제공자가 불명확한 무선랜’

의 조사 결과는 제공자가 불명확하더라도 무선랜을 검색했을 때 보안이 걸려있지 않다면 높은 확률로 사용한다고 응답하였고 보안이 걸려있더라도 단순한 패턴의 암호는 한번쯤 입력해 본다고 응답한 사람이 10%나 되었다.

3. IoT 환경에서 사용자의 보안수용성 향상을 위한 무선공유기 활용도 조사

본 논문에서 조사한 것을 통하여 IoT 환경에서 사용자의 정보보호 인식은 매우 높지만 보안설정을 하지 못하거나 귀찮아서 설정하지 않는 경우도 많이 발생하여 기본적인 보호조치 실행은 미흡하다고 할 수 있다. 또한 보안을 하더라도 WEP보안기술이나 단순패턴의 암호를 사용하여 보안이 취약한 것이 현실이다. 이러한 행동들은 보안의 취약점을 발생시켜 본인뿐만 아니라 남에게도 피해를 줄 수 있다. 실제로 보안이 취약한 가정용 공유기를 이용하여 2014년 11월에 DDos공격을 일으키는 사례도 보고된 바가 있으며, 보안이 허술한 공유기에 침투하여 접속하여 DNS를 위조한 후 해당 공유기를 사용하는 기기들이 인터넷 접속 시 변조된 사이트로 유도하여 개인정보를 해킹하는 방법도 최근 늘어나고 있는 추세이다. 조사항목 중 '제공자가 불명확한 무선랜'에 대해 사용한다고 응답한 사람들은 DNS위조에 노출될 가능성이 상대적으로 크다고 할 수 있으며 그만큼 피해를 입을 가능성이 높다. 현재 상황들을 보면 무선공유기의 보안문제는 기술적인 문제가아니라 사용자의 인식문제라고 볼 수 있다. 본 논문에서 조사한 결과를 토대로 현재 사용자들의 보안수용성을 살펴보면 무선공유기의 보안을 강력하게 사용하는 사용자들이 보안수용성이 높다는 것을 알 수 있고 이것으로 보아 현재의 보안수용성은 매우 저조하다는 것을 알 수 있다. 따라서 보안 문제를 해결하기 위해서는 사용자들의 보안수용성 향상이 가장 중요하다. 무선공유기의 경우 보안수용성을 가장 쉽게 향상 시키는 방법은 암호를 사용하지 않는 44%에 대하여 보안을 할 수 있게 해주는 것이라고 생각한다. 그러기 위해서는 보안설정이 쉬워야 하고 해킹에 대한 경각심을 심어주어 사용자들이 자발적으로 보안을 할 수 있게 유도해야 한다. 국가적 차원에서 사용자들에게 경각심을 심어주고 보안을 조금 더 쉽게 수용 할 수 있도록 대처를 해야 할 뿐만 아니라 사용자본인이 보안에 대한 노력도 많이 해야 할 것이다.

4. 결론

최근 다양한 전자기기들의 등장으로 많은 장소에서 수많은 무선랜이 사용되고 있다. 국가뿐 아니라 기업에서도 서비스를 위하여 무선랜 인프라를 확대해 나가고 있으며 이제 무선랜은 우리생활에서 빼놓을 수 없는 중요한 요소가 되었다. 하지만 사용자들은 무선랜을 사용하면서 보안인식은 높지만 보안수용성은 매우 낮은 경향을 보이고 있기 때문에 본 논문에서는 IoT 환경에서 사용자의 보안수용성 향상을 위한 무선공유기의 활용도 조사를 하였다.

본 논문을 통해 볼 때 IoT 환경에서 사용자들의 정보보호 인식은 매우 높은 반면 보안수용성은 매우 저조하며, 실제로 무선공유기에 대한 비밀번호를 아예 설정하지 않거나 단순한 비밀번호로 설정하는 등 기본적인 보호조치 실행은 상대적으로 미흡하다는 것을 알 수 있다. 이에 사용자의 보안수용성 향상을 위한 본 논문의 결과를 분석하면 다음과 같다. 무선공유기를 사용하는 사용자들 중에서 보안수용성이 낮을수록 비밀번호를 사용하지 않거나 비밀번호의 패턴이 단순할 가능성이 크며, 보안이 취약한 데이터 암호화 기술 방식 사용하거나 제공자가 불명확한 무선랜을 사용하는 비율이 높다. 이를 통해 무선공유기에 대한 보안 기술이 필요하다기 보다는 사용자들의 인식 제고가 먼저 선행되어야 한다는 것을 알 수 있다. 그렇기 때문에 국가적 차원에서 사용자들에게 해킹에 대한 경각심을 심어 사용자의 관심을 이끌어내고 보안설정을 쉽게 할 수 있도록 하여 보안수용성 향상을 하는 것이 가장 적합한 대처라고 생각 한다.

향후 연구에서는 보안수용성의 향상을 위해 어떤 기술로 사용자들에게 더 쉽게 다가가 보안의식을 심어주고 간단하게 보안에 접근하여 설정하게 할 수 있는지 연구해볼 것이다.

감사의글

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터 지원사업의 연구결과로 수행되었음(IITP-2015-H8501-15-1018)

참고문헌

[1] 임재명, 장세정, 김민영, 이정환 "인터넷이용실태조사" 한국인터넷진흥원
[2] 임재명, 장세정, 김민영, 이정환 "모바일인터넷이용실태조사" 한국인터넷진흥원
[3] 임재명, 유지열, 김민영 "무선인터넷이용실태조사" 한국인터넷진흥원
[4] 이승원, 신홍순 "정보보호 실태조사" 방송통신위원회
[5] 이희조, 김효곤, 인호 "무선랜 보안 실태 조사 및 분석을 통한 보안 강화 방안 연구" 고려대학교 학위논문
[6] 정기봉 "무선랜 보안 동향과 대책" 연세 의료·과학기술과 법 제1권 제2호
[7] 백종현, 박순태 "국내 무선랜(WiFi) 보안 운영 현황 및 정책 방향" 정보보호학회지 제21권 제1호
[8] 최구식 "무선보안 무선공유기의 문제점과 확산방지를 위한 제도개선방안" 제284회 정기국회 국정감사 정책자료집
[9] 강유성, 오경희, 정병호 "무선랜 보안기술의 진화동향 및 전망" 전자통신동향분석 제18권
[10] 신동훈, 신동명, 고경희 "무선랜 침해사고 예방대책 연구" 2004년도 한국정보과학회 가을 학술발표논문집 Vol.31, No.2
[11] KIAS 보호나라 http://boho.or.kr/kor/check/check_06.jsp