IOT 환경에서의 사용자 보안에 관한 연구

양현정*, 이창무**
*중앙대학교 융합보안학과
**중앙대학교 산업보안학과
e-mail : {*hj20126, **cmlee}@cau.ac.kr

A Study on User Security in IoT Environment

Hyunjung Yang*, Changmoo Lee**
*Dept of Security Convergence , Chung-Ang University
**Dept of Industrial Security, Chung-Ang University

요 약

최근 사람과 사람, 사람과 사물의 연결에서 일상생활의 모든 것들을 상호 연결시키려는 사물인터넷 기술이 신 성장 동력의 핵심으로 주목받고 확산되어가고 있다. 이러한 IoT 기술의 활성화 및 신규 서비스 창출로 인해 우리의 삶의 질 향상 및 산업 발전을 이루고 있지만 인터넷에 연결된 장치의 수가 증가할수록 이에 수반하는 공격 대상 증가 및 위협 요소도 확장되어 가고 있어 사물인터넷 환경을 안전하게 구축하고 확산하기 위해서는 반드시 사물인터넷에 수반되는 보안적인 이슈를 해결해야 한다. 이러한 해결방안은 단순히 기술적 대응만이 아닌 사용자 스스로가 위협요소를 대처할 수 있도록 사용자 보안 대응방안이 필요하다. 이에 따라 본 연구에서는 IoT 환경에서 발생할 수 있는 위험요소를 도출하고, 이를 토대로 일반 사용자 환경에서 고려해야할 위험요소를 검토해보고 사용자 위협요소는 크게 기술적, 비기술적인 관점으로 구분하여 제시하였다.

1. 서론

최근 웨어러블 디바이스나 셀스케어 서비스, 웹 서비스와 연동된 상황인식 서비스 및 제어 시스템 등 사물인터넷(Internet of Things)이라는 용어로 다양한 제품과 서비스가 개발되고 있다. 사물인터넷은 초연결사회의 기반 서비스 및 기술이자 차세대 인터넷으로 개체 간 인터넷 혹은 사물 간 인터넷으로 정의되며 고유 식별이 가능한 사물이 만들어낸 정보를 인터넷을 통해 공유하는 환경을 의미한다. 사물인터넷은 사물과 사물끼리 센서를 부착해 실시간으로 데이터를 인터넷으로 주고받는 기술이나 환경이다. 사물인터넷이 들어오기 전까지는 인터넷에 연결된 기기들이 정보를 주고받으려면 인간의 '조작'이 개입되어야 했지만, 사물인터넷은 사람의 도움이 없이 인터넷에 연결된 기기들이 서로 알아서 정보를 주고받으며 대화를 나눌 수 있다. 즉, '사람과 사람' 사이의 커뮤니케이션 용도의 인터넷에서 사람의 관계를 뛰어 넘어 사물인터넷으로 인해 '사람과 사물 간' 또는 '사물과 사물 간'까지 활용범위가 확장된 것이다. 이러한 사물 인터넷의 최종 목적은 사람의 개입 없이 사물들이 스스로 알아서 연결되고 소통함으로써 우리의 삶에 편리와 작업의 효율을 증가시키는 것이다.

그러나 사물인터넷 환경은 우리의 삶을 편리하게 만들고 삶의 질을 높여주고 있지만, 사물인터넷에 수반되는 본질적인 보안위험이 계속적으로 증가하고 있다. 단순한 사물인터넷에 발생하는 네트워크 침해의 해킹 공격뿐만 아니라 인간의 프라이버시 침해 같은 윤리적인 문제도 발생될 수 있다. 그렇기 때문에 사물인터넷 환경을 안전하게 구축하고 확산하기 위해서는 반드시 사물인터넷에 수반되는 보안적 이슈를 해결해야 한다. 하지만 현재 사물인터넷이 인간의 개입이 없이 사물과 사물간의 연결을 통해 작동되는 기기라고 생각되어, 대부분의 사람들은 사물인터넷으로 발생되는 위협을 방지하기 위해 사물인터넷 기기 상의 기술적 보안 대처만 실시하고 있다. 그러나 아직 사물인터넷 보안에 대한 기준이 명확하지 않을뿐더러, IoT 제품으로 인해 발생되는 위험이 사용자의 생활 내 발생되기 때문에 사용자 스스로 IoT 보안에 대해 각별히 유의할 필요가 있다.

그래서 본 연구는 새로운 패러다임으로 대두되고 있는 IoT 환경에서 발생할 수 있는 위험요소를 도출하고, 이를 토대로 일반 사용자 환경에서 고려해야할 위험요소를 검토해보고자 한다. 또한 이러한 사용자 환경에서의 위험요소를 방

지 할 수 있는 사용자 중심의 보안방안에 대해 연구해보자 한다.

2. IoT 환경 내 보안 위협요인 도출

본 연구에서는 IoT 환경에서의 적합한 보안 방안을 강구하기 위해 IoT 환경에서 발생할 수 있는 위협요소를 우선적으로 도출하고자 한다. 국 내 IoT 관련 동향분석을 살펴보면, IoT 환경에 수반될 수 있는 위협요인을 다양한 관점으로 설명하고 있다. 한국과학기술기획평가원은 해외의 IoT 환경이 대두되어짐에 따라 이에 발생할 수 있는 기술적 관점의 위협 요소들을 분석하고 대응방안에 대해 제시하였다. 위 연구에서는 IoT 보안 위협에 대해 크게 3가지로 분류하여 설명하고 있다. 첫 번째로 사물인터넷 단말은 고도의 보안솔루션을 도입하기 어렵다는 점이다. 간단한 통신 기능만 탑재된 단말의 경우, 개별적으로 보안 SW를 설치해 구동하는 것이 불가능하고, 보안 HW 모듈을 장착하거나 전체 제어 시스템에 보안 솔루션을 적용하는 등 별도의 노력이 필요하다는 점이다. 두 번째로 외부에서 해킹 사실을 확인 할 수 없다는 점이다. 아직까지 사이버위협에 노출된 사물인터넷 단말을 실시간으로 파악하는 보안 솔루션이 보편화되지 않았으며, 일반 소비자 가전 영역에서는 해킹 공격을 확인할 방법이 전무하다는 점이다. 세 번째로 복잡한 네트워크 구조로 침투 경로가 다양하다는 점이다. 개별 사물인터넷 서비스에서 사용하는 통신 기술 표준이 아직 정립되지 않아 복잡한 네트워크 구조를 형성하고 있으며, 와이파이(Wi-Fi), 블루투스(Bluetooth) 등 이종 네트워크 간 상호 연동 과정에서 일정한 보안 수준 유지 어려움이 발생할 수 있다고 설명하였다. 이외에도 한국인터넷진흥원은 ICT 및 IoT 환경에서 발생 할 수 있는 위협요소에 대해 기술적 위협 요인뿐만 아니라 비 기술적 위험 요인에 대해서도 상세히 설명하고 있다.

위 연구는 기술적 위협 요인으로 목표를 특정하는 Malware 공격이나 모바일 시스템 상에 취약점 공격에 대해 설명하였다. 또한 비 기술적 위협요인으로서 기업의 및 국민의 IoT 사용자 정보보호 인식 부족 및 사회 공학적 방법의 범죄 증가를 제시하였다. 위 연구에서 제시한 IoT 상에서 발생할 수 있는 위험 요소를 다양한 측면으로 요약하면 다음의 (표 1)과 같다.

<표 1> IoT 환경 내 보안위협 요소

	기술 위협요소	비 기술적 위협요소
IoT 위협 요소	o 고도의 보안솔루션 도입 어려움 o 외부 해킹 여부 확인 어려움 o 침투경로 다양성 o APT Mareware 공격	o 사용자 보안 인식부족 o 사회공학 기법 관련 보안범죄 증가

위와 같이 IoT 위협은 단순히 기술적인 요소로만 발생되는 것이 아니라 사용자의 인식 부족으로 인한 기술적인 아닌 부분으로도 발생 될 수 있음을 알 수 있다. 즉, 사물인터넷 단말 기 내 기술적 보안 대처가 완벽하게 구비되어 있어도, 사용자가 보안 소프트웨어를 실행시키지 않거나 제대로 보안패치를 하지 않을 경우에도 보안문제는 발생할 수 있다. 그렇기 때문에 IoT 환경에서 보안 사고를 방지하기 위해서 기술적인 대응방안만 제시하는 것이 아니라 사용자 중심의 보안 대응방안도 마련되어질 필요가 있다.

3. IoT 환경에서 사용자 보안 대응방안

본 연구는 기 도출되어진 IoT 환경 내 보안 위협를 기반으로 사용자 중심의 보안 대응방안을 연구하고자 한다. 위 연구에서 언급한바와 같이 IoT 위협요소는 크게 기술적 위협요소와 비 기술적 위협요소로 구분되어진다. 그렇기 때문에 사용자 보안도 이러한 두 가지 위협요소의 관점으로 구분하여 제시하고자한다. 기술 위협요소의 대응방안 중 첫 번째는 IoT 제품/서비스의 취약점 보안패치 및 업데이트이다. IoT 단말기는 IoT 제조사와 서비스 제공자가 안전 IoT 제품 개발 및 서비스 이용환경을 조성하기 위해 해당 서비스에 대해 정확히 이해하고, IoT제품과 서비스의 설계 단계에서부터 제품 및 서비스가 적용될 환경을 기반으로 보안취약점을 사전에 분석하여 이를 보완하고 강화할 수 있는 기술을 적용하였다.

하지만 완벽한 보안 플랫폼이 장착된 사물인터넷 단말기라도 신규 바이러스가 끊임없이 발전하고 확산되어짐에 따라, 사용자는 이러한 신규 바이러스에 대한 대처를 위해 주기적으로 보안패치를 수행해야한다. 사용자는 주기적으로 보안패치 버전을 확인하고 최신패치로 업그레이드하거나 자동으로 업데이트가 되도록 설정해야한다. 두 번째로 IoT 단말기 비밀번호 관리이다. 현재 IT를 사용하는 대부분의 사용자들은 해당 기기의 관리자 ID 및 비밀번호를 디폴트 ID와 비밀번호로 설정하는 사람이 많다. IoT 단말기는 그 자체가 IP주소를 갖고 있기 때문에 해커들은 네트워크를 통해서 불법적으로 단말기로 접근할 시 이를 방지할 수 있는 것은 인증 관리밖에 없다. 그렇기 때문에 사용자는 IoT 단말기 설치 즉시 기본 사용자 이름과 비밀번호를 변경하고, 이를 정기적으로 바꿔 보안수준을 향상시켜야한다.

다음으로 비 위협요소의 대응방안은 사용자의 보안인식 제고이다. 아직까지 IoT를 포함한 인터넷 및 모바일을 이용하는 사용자의 보안인식이 많이 부족하다. 이러한 보안인식을 재고하기 위한 가장 좋은 방법은 보안교육이다. 그렇기 때문에 IoT의 안정적인 확산을 위해 반드시 학교에서나 직장에서 IoT 관련 보안교육을 실시해야 한다. 또한 IoT 서비스 제공자는 IoT 단말기 및 서비스를 제공 할 시 제품 관련 보안사항에 대해 사용자에게 알려줘야 하고 제품설명서에도 이를 명시해야한다. 사용자도 설명서에 나온 보안지시사항을 이행하고 보안패치 및 업데이트 등과 같은 주기적으로 수행해야하는 보안조치사항을 수행해야한다.

4. 결론

최근 사람과 사람, 사람과 사물의 연결에서 일상생활의 모든 것들을 상호 연결시키려는 사물인터넷 기술이 신 성장 동력의 핵심으로 주목받고 확산되어가고 있다. 이러한 사물 인터넷은 사람의 개입 없이 사물들이 스스로 알아서 연결되고 소통함으로써 우리의 삶에 편리와 작업의 효율을 증가시켜가고 있다. 하지만 IoT 기술의 활성화 및 신규 서비스 창출로 인해 우리의 삶의 질 향상 및 산업 발전을 이루고 있지만 인터넷에 연결된 장치의 수가 증가할수록 이에 수반하는 공격 대상 증가 및 위협 요소도 확장되어가고 있다. 사물인터넷의 위협은 현재 단순한 경제적 피해를 넘어서 인명 피해가 유발될 수 있기 있으며, 주변의 일상 사물들이 연결되어짐에 따라 개인 정보 유출이나 프라이버시 침해가 우려된다. 그렇기 때문에 사물인터넷 환경을 안전하게 구축하고 확산하기 위해서는 반드시 사물인터넷에 수반되는 보안적 이슈를 해결해야 한다. 그리고 단순히 기술적 대응방안만이 아닌 사용자 스스로가 위협요소를 대처할 수 있도록 사용자 보안 대응방안이 필요하다.

이에 따라 본 연구에서는 IoT 환경에서 발생할 수 있는 위험요소를 도출하고, 이를 토대로 일반 사용자 환경에서 고려해야할 위험요소를 검토해보았다. 사용자 위협요소는 크게 기술적, 비기술적 관점으로 구분하여 제시하였다. 그리고 이를 토대로 IoT 환경 내 보안 수준을 향상 시킬 수 있는 사용자 보안 대응방안을 제시하였다. 본 연구는 IoT 사용자가 단순히 보안문제를 기술적인 문제로만 인식하지 않고 능동적으로 수행해야한다는 보안인식 재고에 기여할 수 있을 것이라고 생각한다.

참고문헌

[1] 한국과학기술기획평가원, IoT 보안 위협 동향, 2015

[2] 이용규, 윤구홍, 사물인터넷(IoT) 산업 진흥을 위한 정부의 역할에 관한 연구 - AHP를 활용한 정책 중요도 분석을 중심으로, 디지털융복합연구, 14, 5, 47-55.

[3] 김기웅, 권창희, 중소기업의 IoT관련 정부 R&D 현황 및 정책적 시사점. 정보기술아키텍처연구, 13, 3, 431-443

[4] 원유재, IoT(Internet of Things) 정보보호 기술 개발 방향, 32, 1, 24-27