사물인터넷(IoT) 보안 기술 동향

김진석*, 전문석*
*숭실대학교 컴퓨터공학과
e-mail:dooleya@ssu.ac.kr

Technology Trends for Internet of Things Security

Jin-Seok Kim*, Moon-Seog Jun*
*Dept of Computer Science & Engineering, Soongsil University

요 약

사물인터넷은 각종 사물에게 통신 기능 및 센서 기능 장치를 부착하여 인터넷에 연결될 수 있게 하고 각 사물들 간에 통신을 가능하게 하는 기술을 의미한다. 미국의 국가정보위원회는 2025년까지 다양한 분야에서 국가경쟁력에 영향을 미칠 수 있는 6대 기술 중 하나로 사물인터넷을 꼽고 보안 대책을 마련하고 있다. 여러 분야에 걸쳐 있는 사물인터넷의 보안 대책 수립을 위해 각 분야별로 다른 접근법을 제시하는 것이 필요하다.

1. 서론

사물인터넷(Internet of Things, IoT)은 각종 사물에게 통신 기능 및 센서 기능 장치를 부착하여 인터넷에 연결될 수 있게 하고 각 사물들 간에 통신을 가능하게 하는 기술을 의미한다. 1970년대에는 전세계의 컴퓨터가 인터넷을 통해 연결되기 시작하였다면 1990년대에는 문서 및 데이터와 상호 지식을 교류하기 위한 웹이 등장하였으며 이는 21세기 사물인터넷 시대에 이르러 모든 사물들이 인터넷에 연결될 수 있게 하는 기반을 제공하였다.

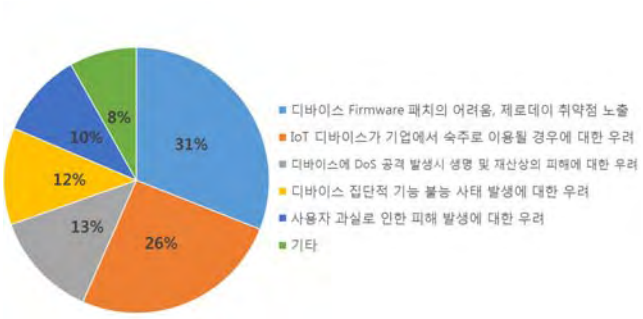
미국의 정보 기술 연구 및 자문회사이자 시장조사기관인 가트너(Gartner)에 따르면 2009년까지 사물인터넷 기술을 사용하는 사물의 개수는 9억 개였으나 2020년에는 약 260억 개에 이를 것으로 예상하고 향후 10년간 유망할 것으로 생각하는 미래 IT분야로 IoT를 선정하였으며, 시스코 시스템즈(Cisco Systems)의 조사에 따르면 2013년부터 2022년까지 10년간 사물인터넷이 14조 4천억 달러의 경제적 가치가 있을 것이라고 예상하고 있다.

하지만 사물인터넷이 발전함에 따른 보안의 중요성 역시 간과할 수 없는 부분임에 틀림없다. 모든 사물들이 인터넷에 연결되고 통신한다는 것은 곧 사물들에 대한 공격자의 침투 가능성이 높아진다는 의미이기도 하다. IoT 서비스에 보안 문제가 발생하면 서비스 제공 불가에 대한 부분뿐만 아니라 사용자의 안전까지 위협받을 수 있다.

따라서 본 논문에서는 사물인터넷에 대한 취약점 및 보안 기술 동향에 대해 살펴보고자 한다.

2. 사물인터넷(IoT)의 취약점

노튼(Norton)백신으로 잘 알려진 보안업체 시만텍(Symantec)은 IoT기술이 보편화됨에 따라 발생할 수 있는 해킹 가능성에 대해 지적하였다. 다수의 IoT 기기가 사용하는 리눅스 기반의 운영체제의 경우 제때 업데이트가 이루어지지 않거나 적절한 보안 기능을 가지지 못할 경우 리눅스 웜에 의해 해킹당할 위험이 존재한다.

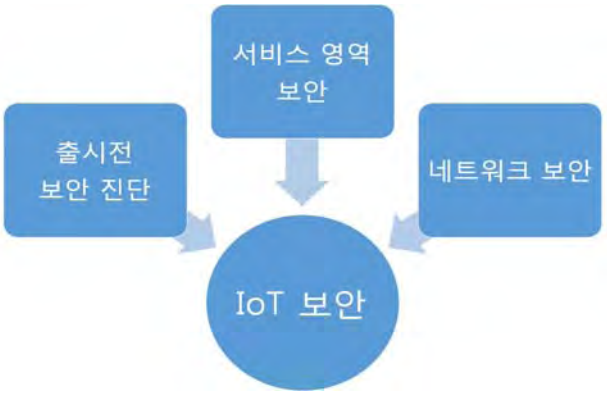


(그림 1) IoT 위협통계

실제로 2013년 10월경 러시아에서는 중국산 주전자, 다리미에서 무선네트워크 접속 및 도청 기능이 탑재된 칩셋이 발견되었다. 약 200미터 근방에 보안기능이 없는 무선네트워크에 침투하여 연결된 컴퓨터로 바이러스를 전송한 후 도청 가능한 환경으로 만들게 하는 장치였다. 같은 해 8월에는 조명기기 회사 필립스(Philips)에서 출시한 LED 전구 제어시스템을 해킹 시연하기도 하였다. 이 시연을 통해 전구 제어기기에 대한 취약한 보안을 무력화시킬 수 있음을 보였다. 이밖에도 스마트 TV등을 해킹하여 자유자제로 원격제어를 하고 악성 어플리케이션에 감염된 스마트폰을 조작하여 수십만 건의 스팸 메일을 전송하는 등 사물인터넷 보안 침해 사고는 끊이지 않고 있다.

<표 1> IoT 디바이스 공격 유형 분석

공격명	설명
Interference/ Jamming/Collision	주파수 위변조 등을 통해 실제 신호의 정상적인 송수신을 방해하는 공격
Sybil	센서네트워크에서 Multi-Identity가 허용되는 취약점을 이용한 공격
Traffic Analysis	암호화되지 않은 NPDU, DLPDU 페이로드를 분석하여 정보를 취하는 공격
DoS	지속적인 광고 패킷을 송신, CRC 반복 체크로 시스템에 무리를 주거나 주파수 Jamming 등을 통해 신호 송수신을 방해하는 공격
De-synchronization	잘못된 시간 정보를 송신하여 디바이스가 계속적으로 자원을 소모하도록 하는 공격
Wormhole	통신 라우팅을 고의로 변경하거나 악성코드 배포 경로로 이용하는 공격
Tampering	단말에 저장된 데이터 혹은 송수신 데이터를 임의로 위·변조하는 공격
Eavesdropping	암호화되지 않은 디바이스(센서)-Gateway 구간 정보를 도청하는 공격
Selective Forwarding Attack	특정 노드로의 패킷 포워딩을 막아 해당 노드를 Blackhole로 만들어버리는 공격
Spoofing	허가되지 않은 디바이스를 네트워크에 접속시켜 악의적인 행위를 하도록 하는 공격



(그림 2) IoT 보안 대책

3. IoT 보안 대책

3.1 출시 전 보안 진단

제품의 보안 취약점이 조기에 발견되지 않는다면 서비스를 제공하는 회사의 입장에서는 사고 발생 시 금전적인 손실에 대한 보상이 필요할 수 있다. 사고의 여파가 막대하거나 사회적으로 큰 문제일 경우 기업의 입지가 흔들릴 수도 있다. 따라서 IoT 제품과 서비스를 제공하는 회사는 출시 전부터 제품의 보안에 대한 검사를 철저히 하여 사고를 미연에 방지해야 한다.

3.2 서비스 영역 보안

서비스 영역에서는 제품의 등록, 제품에 대한 사용자 인증, 사용자 권한 설정 등의 정보를 진단한다. 제품에는 고유의 식별자가 부여되며 사물인터넷과 연결하기 전에 서버에 등록되어야 하고 연결 시 사용자 인증과 권한 여부를 검사하게 된다.

사물 간 정보를 전송하는 구간에 대해서도 암호화가 필요한데 주로 사용되는 SSL(Secure Socket Layer) 암호화의 경우 상호인증 부재의 문제점이 있다. 이러한 경우를 방지하기 위하여 안전한 SSL 프로토콜을 사용하고 송·수신자간 인증 여부를 확인해야 한다.

3.3 네트워크 보안

네트워크는 TCP/IP 뿐만 아니라 무선 네트워크도 포함된다. 즉, 무선 네트워크를 사용하는 기술인 지그비(Zigbee), 와이 파이(Wi-Fi)등도 보안 점검이 필요하다.

지그비의 경우 각각의 장치는 장치 자신에 대한 신뢰성을 보장한다. 즉, 지그비간 통신과정에서의 보안이 보장된다면 신뢰할 수 있는 통신이 된다. 하지만 모든 구간에서의 통신이 암호화 되는 것은 아니기 때문에 적절한 대책 마련이 필요하다.

와이 파이의 경우 인가되지 않은 사용자의 접근과 패킷 스니핑, 정보 유출 및 위·변조 등에 대해 매우 취약한 것으로 알려져 있다. 따라서 패킷을 송·수신하는 사물들 간 인증과 암호화가 이루어져야 한다.

4 결론

미국의 국가정보위원회는 2025년까지 다양한 분야에서 국가경쟁력에 영향을 미칠 수 있는 6대 기술 중 하나로 사물인터넷을 꼽고 보안 대책을 마련하고 있다. 백악관에서는 2013년 2월 국립표준기술연구소의 주도 하에 사이버 보안 프레임워크를 수립하였고 미국 식품의약청(FDA)에서는 의료장비에 대한 보안 지침을 마련해, 이를 준수하지 않은 제품은 미국 내에서 판매 및 유통을 금지하였다.

유럽의 경우 2014년 9월 유럽데이터보호 감독기구 작업반 29(Working Party 29)에서 사물인터넷 데이터 보호와 관련된 권고안을 발표하였다.

미래창조과학부는 2014년 10월경 '사물인터넷 정보보호 로드맵'을 발표하고 정책을 추진 중에 있다. 또한 정부가 제시하는 사물인터넷 보안 기준을 업계에 확신시키고자 정부와 기업 협력 하에 민관합동기구 '사물인터넷 보안 협의체'를 구성 및 운영하고 있다.

사물인터넷은 그 범위가 매우 넓어 이에 대한 보안 대책 수립이 까다롭다. 또 각 산업 분야별로 보안 위협요인과 대응이 달라지기 때문에 일관된 보안 기준을 결정하기 어렵다. 따라서 각 분야별로 보안 체계를 갖추기 위해 별도의 기준을 마련해 접근하는 것이 필요하다. '사물인터넷 정보보호 로드맵'과 같이 사물인터넷 정보보호 정책의 국가적 추진이 더욱 중요할 것으로 예상된다.

참고문헌

[1] 김기환, 김대철, 신용태 "사물 인터넷(IoT) 동향 및 차세대 보안 기술방안 연구" 2015년도 한국인터넷정보학회 추계학술발표대회 논문집 제16권2호

[2] 진한나, 박석천, 최원태 "사물인터넷(IoT)의 네트워크 보안기술 분석" 2014년도 한국인터넷정보학회 추계학술발표대회 논문집 제15권2호

[3] 공만식, 채홍준, 유보현 "사물인터넷(IoT) 기술동향과 전망" 기계저널 THEME 01

[4] 표철식, 강호용, 김내수, 방효찬 "IoT(M2M) 기술동향 및 발전 전망" 한국전자통신연구원