1. 개요

온라인 기기의 무선 네트워크를 기반으로 방송·통신·인터넷 등 개별 지능화된 디지털기기의 미디어 간 통합을 통하여 사람뿐만 아니라 사람-사물, 사물-사물까지 통신의 영역이 확대되고 있다. 또한 이를 활용한 다양한 콘텐츠와 개인 맞춤형 통합서비스가 확산되고 있으며 스마트폰에서 이용하는 교통, 위치정보, 기상정보 등이 다 양한 사례이다.

이와 같은 현상은 현대 사회를 사람과 사물, 자연, 사이버 세계 등 모든 객체가 스마트 기기와 통신 네트워크를 통하여 언제 어디서나 원하는 형태로 상호 연결될 수 있는 초 연결 사회로 이끌고 있다. 아울러 통신에 기반 한 초 연결 사회는 미래의 새로운 경제 상장 동력으로 부상하고 있으며 핵심 기술은 사물인터넷 (IoT: Internet of Things)이다.

사물인터넷이는 미래 인터넷의 통합된 부분으로써 표준과 상호 호환 통신 프로토콜로 자가 설정 기능을 갖춘 동작 글로벌 네트워크 인프라이며 자기식별자와 각각의 특성을 갖는 물리적인 사물과 가상 사물로 CERP-IoT 2009에서 정의하고 있다.

IoT는 자율적으로 물리적인 실 환경에 반응하는 기기의 직접적인 개입 유효성을 필요없이 서비스를 만들거나 특정 행위를 하는 프로세스를 실행한다. 즉, 인간과 주변 환경과의 상호 연결을 위해 실시간 기술과 각종 유무선 네트워크 기술을 사용한다.

정리하면 상황 인지 소프트웨어 오픈 플랫폼 기술, 웹 서비스 기술 그리고 소셜 네트워크에 의해 가장 또는 처리되어 사물 간의 자율적 통신 기반가능한 사물통신 (M2M: Machine to Machine) 개념이 무선통신을 넘어 인터넷 구조상에 적용됨으로써 현실과 가상계의 모든 정보와 상호작용하는 개념으로 전환된 차세대 인터넷 환경을 의미한다.
현재, IoT는 다양한 산업 분야에 적용되고 있으며 우리 생활과 밀접한 홈·가전, 의료, 교통 분야에서 본격적인 시장 활성화가 진행 중이다.

Gartner는 매년 발표하는 하이프 사이클(SJ(Hype Cycle))에서 최단 유망 기술에 대한 전망으로 2012년부터 2014년 가장 주목해야 할 10대 전략 기술 가운데 하나로 사물인터넷을 선정하였다. 또한 PC, tablets와 스마트폰을 제외한 인터넷에 연결된 기기가 2009년 9억 대 수준에서 2020년에는 2009년 대비 30배가량 증가한 260억 대가 될 것이라고 전망하였다(1).

IoT 서비스가 일상생활로 확산되면서 기존 사이버 세계에서의 여러 가지 위협 요소들이 현실 세계로 전이 확대되고 있다. 사물에 인터넷 기능이 추가됨에 따라 보호해야할 기기의 수가 우리 일상생활의 모든 사물로 확대되고 장단점, 올림픽, 조연결성 등의 특성에 따라 암호화, 인증 및 이 기종 네트워크 보안 관리, 사생활 보호 및 보안 기술 적용에 한계가 존재한다.

또한 사물인터넷 통신상에서 발생될 수 있는 정보유출, 데이터 위변조, 복제 공격, 서비스 거부, 사생활 침해 등의 보안 위협 역시 크게 증가하므로 제품과 서비스의 기획 및 설계단계부터 정보보호를 고려하여야 하며 기존의 제조업, 서비스업 등 전 산업 분야에 IoT 보안을 표준화 할 필요가 있다(2).

본 기고에서는 이러한 맥락에서 IoT 환경에서의 보안 위협 요소를 살펴보고 IoT의 기술요소 및 동향, 표준화 방향을 설명하며 보안 구현 사례로 (주)CIOIT에서 개발한 IoT 보안 기술을 살펴보면서 IoT 보안에 대한 안전성 확보를 위한 보안 전략에 대한 하나의 방향을 제시하고자 한다.

2. 보안 관련 기술

2.1 보안 위협 요소

2.1.1 유무선 단말기

단말기의 기능 및 종류들의 다양화 및 저 사양 단말기의 증가에 따라 단말기에 백신, 암호화, 인증 및 보안을 적용하기가 어려워지고 단말기의 관리 및 모니터링의 어려움이 발생하고 있다. 따라서 저 사양의 단말기 및 다양한 단말기의 특성을 고려한 백신, 암호화 그리고 인증에 대한 정량 보안 기술의 개발 및 적용이 필요하다.

2.1.2 네트워크

ZigBee, Wi-Fi, Bluetooth 등의 이중무선 네트워크 간 상호 연동 상에서 보안은 통신 지역에 따른 지역이 발생하면서 인증에 대한 제한이 따르는 등 위협요소를 내포하고 있다. 또한 클라우드 컴퓨팅 환경에서 대량의 중비 클라우드를 통하거나 네트워크상에서 연동되는 홈 가전 또는 의료기기 등에 악성코드를 감염시켜 네트워크 트래픽을 폭 증시감으로써 네트워크 성능을 저하시키는 등의 위협 요소를 갖고 있다. 따라서 이 기종 망 연동을 위한 보안기술 및 대규모 기기 및 네트워크에 대한 보안 기술의 적용이 필요하다.

<table>
<thead>
<tr>
<th>구분</th>
<th>위협요소</th>
<th>대안</th>
<th>기타</th>
</tr>
</thead>
<tbody>
<tr>
<td>단말기</td>
<td>데이터 위조 및 변조, 비인가된 접근</td>
<td>LEA, HIght, PRESENT, KATAN</td>
<td>여전히 해당됨</td>
</tr>
<tr>
<td>네트워크</td>
<td>신호 데이터의 가해성, 무결성, 침해, 서비스 가해, 정보 유출</td>
<td>동신 프레임 보안 및 카 설정, TKIP, CCMP</td>
<td>여전히 취약</td>
</tr>
<tr>
<td>플랫폼서비스</td>
<td>비인가된 서비스 및 사용자 접근</td>
<td>Authentication Component</td>
<td>-</td>
</tr>
</tbody>
</table>

(표 1) 보안 위협 요소