

인터넷을 통해 이와 같은 스마트 사물과의 상호 작용을 촉진하고 보안과 프라이버시 이슈를 고려하여 사물의 상태나 관련 정보를 질의 혹은 교환한다라고 정의되고 있다.

앞의 정의를 보면 사물이라는 것이 물리적인 사물과 가상적인 사물을 모두 포함하는 개념이라는 것을 알 수 있는데, 여기서 언급된 가상적인 사물의 예로는 소프트웨어 서비스, 소프트웨어 객체, 행위 주체로서의 액터(Actor) 등이 있다. 또한, 지능형 인터페이스는 통신/네트워크, 프로토콜 관점뿐만 아니라, 상황이나 어떤 정보를 인식하는 것도 인터페이스라고 볼 수 있다. 또한, 정의의 마지막 부분에서는 사물인터넷에서의 보안과 프라이버시의 중요성을 언급하고 있는데, 신뢰할 수 없는 사물인터넷 제품과 서비스는 절대 시장에서 활성화되기 어려울 것이며, 당연한 것으로 보인다. 본 고에서는 사물인터넷의 보안 취약성을 살펴보고 이러한 보안 취약성에 대한 보안 기술도 살펴보고자 한다.

2. 사물인터넷 보안 취약성

2.1 사물인터넷 보안 취약성

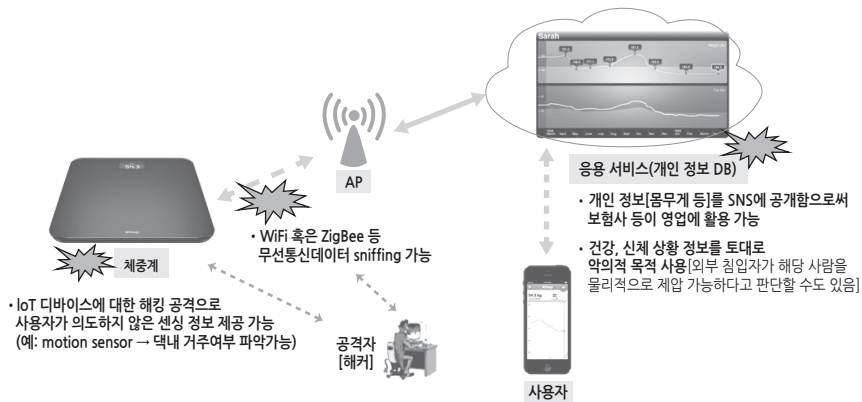
사물인터넷은 여러 가지 요소기술이 통합되어 특정 서비스를 구성하기 때문에 각 요소 기술 자체의 보안 취약성과 연동 시 새로운 보안 취약성 발생할 가능성이 매우 높다. 즉 사물인터넷은 정보를 센싱하기 위한 센서 기술과 센싱된 정보에 대한 원활한 통신/네트워킹을 위한 기술, 사물인터넷 디바이스 자체를 위한 칩 기술, 기능 구현을 위한 OS 기술/임베디드 시스템 기술, 디바이스의 자율 동작과 지능적 동작을 위한 플랫폼 기술, 대량의 데이터를 처리하는 빅데이터 기술, 유용한 정보 추출을 위한 데이터 마이닝 기술, 사용자 중심의 사물인터넷 서비스를

위한 웹 서비스/응용 서비스/WoT(Web of Things) 기술 등 다양한 형태의 기술이 사용되어 사물과 사람, 서비스가 통합된 사물인터넷 서비스가 실현된다. 이를 구성하는 각 요소 기술의 보안 기술은 디바이스나 OS 기술, 통신/네트워킹, 웹 서비스/응용 서비스 등에서는 기밀성, 무결성, 인증, 접근제어, 해킹 방지, Anomaly 탐지/대응 등 다양한 보안 기술이 많이 개발되어 사용되고 있다. 또한, 데이터마이닝이나 빅데이터 기술 분야에서는 프라이버시 보호 중심으로 다양한 기술이 개발되어 사용되고 있다.

한편, 사물인터넷은 언급한 것처럼 다양한 기술의 복합적 특성 외에, 사물인터넷 서비스가 기존의 서비스와 다른 특성을 가진다. 즉, 기존의 응용 서비스는 단일 사업자가 주도하는 vertical application market이었지만, 사물인터넷 서비스는 다양한 주체가 공존하는 horizontal market 특성을 가진다. 이 때문에 여러 주체 간 프라이버시 보호 책임과 권한 선정의 어려움이 생긴다. 즉, 사물인터넷 환경은 센서 디바이스 공급자와 통신/네트워크 공급자, 서비스 개발자, API 개발자, 플랫폼 공급자, 데이터 소유자 등 다양한 주체가 존재하기 때문에 보안/프라이버시 보장이 어렵게 되는 것이다. 물론 프라이버시를 보장하는 기술은 프라이버시 보호를 위한 법이나 체계에서 프라이버시 보호를 위한 범위 및 대상을 명확히 정의해야 하는데, 현재 개인정보보호법(한국)과 Consumer Protection/Data Protection Act(미국)에서는 사물인터넷 환경에 적용 가능한 구체적인 프라이버시 보호 체계가 정의되지 않았다는 문제가 존재한다.

2.2 사물인터넷 보안 취약성 사례

본 절에서는 시중에 나와 있는 사물인터넷 제품(서비스)에 대한 보안/프라이버시 침해 상황을 분석함



[그림 1] 사물인터넷 제품(체중계) 사례에서 본 보안 취약성

으로서 사물인터넷 보안 취약성을 이해하고자 한다.

[그림 1]은 체중계가 인터넷에 연결되고 각종 분석 기능과 다양한 서비스와 연동이 가능한 사물인터넷 제품/서비스 사례를 보여주고 있다. 사용자가 측정한 체중 정보는 서비스 제공업체의 클라우드에 전송되며 해당 정보를 사용자는 스마트폰과 같은 단말에서 앱을 통해 확인할 수 있다. 언급한 체중 정보 흐름은 단순해 보이며 서비스도 단순해 보이지만 개인의 체중 정보는 매우 다양한 형태의 서비스에 활용될 수 있다. 예를 들어, 어떤 사물인터넷용 체중계는 측정한 개인의 체중 정보를 개인의 선택에 따라 트위터와 같은 SNS에 업로드할 수 있다. 이는 공개된 정보이므로 보험회사에서 해당 정보를 활용하여 사용자에게 맞춤형 보험 상품 판매 업무를 할 수 있다. 또한, 이미 보험 가입자라면 체중의 변화에 따라 건강 위험도의 변화로 인식하여 자사의 보험 손실을 우려하여 해당 사용자에게 영향력을 미치고자 할 수도 있을 것이다. 아울러, 서비스 업체에 저장된 개인의 체중 정보가 악의적인 목적으로 사용될 수도 있으며, 서비스 업체가 자사의 이익을 위해서 분석/가공을 통해 회사 입장에서는 부가가치가 높은 다른 정보로 변환할 수도 있을 것이다.

어떤 경우에도 원래의 데이터 소유 주체의 의사에 반하는 형태로 데이터가 활용되는 것이므로 프라이버시 침해가 발생하게 되는 것이다.

그런데 만약 이런 상황에서 체중계 사용자(체중 정보 소유자)가 자신의 정보에 대한 통제권을 확보하고자 하는 경우, 현재의 사물인터넷 서비스 환경에서는 쉽게 자기정보통제권을 얻을 수 있을지 의문이다. 예를 들어, 만약 업체에서 자사가 보유하고 있는 정보를 가공하여 제3의 업체에 판매한 경우, 판매 이후에는 정보를 제공한 업체에서는 해당 사용자의 정보를 통제할 수 없을 것이며, 가공된 정보는 원래의 정보라고 볼 수 없기 때문에 최초의 체중 정보 소유자가 이 경우에 해당 정보에 대한 통제권을 가진다고 볼 수도 없게 된다. 지금까지 단일 업체에 의한 정보 처리 및 관리가 이뤄졌고 사물인터넷 환경처럼 여러 주체가 관계되는 경우는 없었기 때문에 기존의 프라이버시 관련 법과 체계는 새로운 사물인터넷 환경에 맞게 정비될 필요가 있다.

언급한 프라이버시 침해 가능성 뿐만 아니라 [그림 1]에서 보듯 체중계에서 센싱되어 무선 통신 채널로 전송되는 정보를 악의적인 공격자가 가로챌다면(sniffing), 공격자는 해당 정보를 활용하여

사용자의 신체적 특성을 유추하여 이를 악의적인 목적에 사용할 수 있을 것이다. 많은 사물인터넷 디바이스와 플랫폼에는 접근 제어, 인증/인가 기술에 있어서 높은 등급의 기술이 구현되지 않기 때문에 상대적으로 공격에 취약하다. 만약 체중계에 motion sensor가 있다면 공격자는 취약한 보안 체계를 뚫어서 해당 센서에 대한 제어권을 확보하여, 개인의 체중 정보 뿐만 아니라, 맥내 거주 여부도 쉽게 알 수 있게 된다. 이처럼 사물인터넷 제품과 서비스에서는 각별히 보안과 프라이버시 침해 문제를 살펴볼 필요가 있다.

3. 사물인터넷 서비스 보안

2장에서는 사물인터넷의 보안 취약성과 프라이버시 침해 가능성에 대해 살펴보았다. 기존의 단일 업체가 책임지는 Vertical Market 응용 서비스와 달리 사물인터넷의 다양한 주체의 개입에 의해 보안 취약성 해결과 프라이버시 침해 문제 해결이 쉬운 문제가 아닌 것을 확인했다. 사물인터넷의 구성 요소 기술 및 특성 중에서 통신/네트워크 보안 기술(CoAP, MQTT 보안 등)이나 Open API 보안 기술(OAuth 등), 플랫폼 보안, 서비스 보안 기술, 해킹 대응, OS 보안, 접근제어, 인증/인가, Anomaly Detection 등 System 보안 기술 등은 기존의 보안 기술을 활용하거나 이미 정의된 보안 기술이 존재하기 때문에 비교적 다루기 용이한 사물인터넷 보안 기술로 보인다. 하지만, 프라이버시 보호와 디바이스/서비스/데이터에 대한 통합 보안 기술, Security Anchor 기술 등은 앞으로 지속적인 연구가 필요하다. 본 장에서는 사물인터넷 보안 기술 중에서 서비스에 대한 보안 기술을 살펴본다.

사물인터넷 서비스는 다양한 디바이스와 플랫폼,

데이터 소유 주체, 그리고 다른 응용 서비스를 활용하여 새로운 서비스가 만들어지는 구조를 갖는다. 이 때문에 인증/인가 기법, 접근 제어/권한 제어 기법, ID(Identification) 관리 기법, 키 관리 및 분배 기법, 신뢰 제어 기법 등 다양한 보안 기법을 필요로 한다. 사물인터넷 서비스 보안 기술과 관련하여 IoT-A 프로젝트[1]에서 정의한 보안 기술을 살펴보기로 한다. IoT-A 프로젝트에서는 인증을 위해 AuthN이라는 컴포넌트를 정의하였고 인가를 위해서는 AuthZ(Authorization) 컴포넌트, ID 관리를 위한 IM, 키 교환 및 관리를 위한 KEM(Key Exchange and Management), 신뢰도 및 평판 관리를 위한 TRA(Trust and Reputation) 컴포넌트를 정의하고 있다.

일반적으로 인증을 위해서 패스워드와 같은 지식 기반 인증, 스마트카드와 같은 소유 기반 인증, 그리고 지문과 같은 생체정보 기반 인증이 가능한데, IoT-A 보안 기법에서는 특정한 인증 기법 사용을 의무화하지 않고 상황에 따라 다양한 인증 기법 사용을 권하고 있다. 예를 들어, 사전 공유 비밀정보를 사용한 객체 간 인증도 가능하며, 공개키 인증서(certificate)를 사용한 객체 간 인증도 가능할 것이다. 사용자인 경우, 사용자 ID와 패스워드 기반 인증도 가능할 것이다. 사용하는 인증 기법에 대한 적절한 키 분배 및 관리 기법도 필요하다[2]. 인증 과정은 AuthN 컴포넌트에서 실현되는 것으로 정의되어 있다.

인증 과정을 거친 후, 해당 자원에 대한 사용 권한을 확인하여 권한을 부여해주는 것을 인가(Authorization)라고 하며, IoT-A에서는 이를 AuthZ 컴포넌트에서 수행한다. 또한, 접근 제어 대상 자원에 대한 접근이 발생할 때마다 해당 접근이 허용되는지 여부를 확인받아야 하는데 이 부분도


AuthZ 컴포넌트에 의해 이뤄진다. 사물인터넷에서는 접근 대상 자원이 어디에 있는 지를 찾는 기능(Resolution)이 필요한데, 이 Resolution 기능 수행 후, 해당 자원에 대한 접근 권한이 있는 지를 확인해야 하므로 인가 기능이 수행되는 것이 일반적이다. 여기서 접근 권한은 다양한 접근 제어 기법을 사용할 수 있지만, 사물인터넷과 같은 복잡한 시스템 적합한 접근 제어 기법으로는 RBAC(Role Based Access Control)이나 ABAC(Attribute Based Access Control)이 좋다. 이는 역할 단위 혹은 속성 단위의 접근 제어가 가능하여 서비스 객체와 같은 다양하고 복잡한 미세 단위의 접근 제어가 필요할 때 사용한다.

사물을 다른 사물과 구별하고 식별하기 위해서 식별자 관리(Identity Management: IM)가 필요하다. 하지만 식별자는 프라이버시 침해의 기본 이유가 된다. 예를 들어, 특정 사용자가 특정 사물(서비스)을 사용하는 정보가 공개된 경우 해당 정보는 사용자의 프라이버시를 침해할 가능성이 있는 것이다. 프라이버시라는 것은 사람이 아닌 사물에는 존재하지 않지만, 사람과 연관되어 있거나 연결시킬 수 있는 경우에는 프라이버시 침해가 되기 때문에 보호 대상이 되는 것이다. IM 컴포넌트에 프라이버시 보호를 위해 익명화(Anonymization)과 별명화(Pseudonymization)를 적용할 수가 있다. 한편 만약 어떤 서비스 식별자를 Pseudonym을 사용하여 다른 식별자로 바꿔 프라이버시를 보호하고자 하는 경우, 해당 식별자의 변경 여부와 어떤 식별자가 어떻게 변경되었는 지를 지속적으로 추적 및 관리할 수 있어야 하며 이를 위한 관리 기법이 필요하다.

인증 과정에서 Credential 값을 사용하거나 공개 키 인증서, 비밀번호 등을 사용할 경우 이에 대한 관리가 필요하다. 이를 위해서 IoT-A에서는 KEM

컴포넌트가 제공되는데 일반적으로 암호 기법을 사용할 때는 키 관리가 중요한 이슈이다. 또한, 사물인터넷 서비스에서는 해당 서비스가 믿을만한 것인지 해당 디바이스에서 센싱되어 전송된 정보가 오류가 없는 센싱값인지를 판단하고 관리하는 메커니즘이 필요하다. 센서는 센싱 단계 혹은 전송 단계에서 오류를 유발시킬 수 있으므로 이에 대한 신뢰도 관리가 필요하다.

4. 맺음말

본 고에서는 사물인터넷이 기존의 응용 서비스와는 달리 Horizontal Market 특성을 가지며 여러 요소 기술의 복합체이고 관련 있는 주체가 다양하다는 사실을 살펴보았다. 이러한 사물인터넷의 특성에 의해 보안 취약성과 프라이버시 침해 문제는 더욱 해결하기 어렵고 복잡한 문제로 인식되고 있다. 사물인터넷 보안 기술을 살펴보기 위해 IoT-A 프로젝트에서 정의한 보안 기술을 살펴보았는데, IoT-A 프로젝트에서는 주요 보안 기술로 인증과 인가, 접근 제어, 키 관리, 식별자 관리, 신뢰도 및 평판 관리 기법을 언급하고 있다. 하지만, IoT-A에서 정의한 보안 기술도 기본 틀 정도만 제시하고 있으며 자세한 내용은 정의되지 않았다. 또한 프라이버시 보호에 대한 내용은 거의 언급되지 않고 있기 때문에 향후 사물인터넷 활성화를 위해서 이에 대한 많은 연구가 필요하다. 

[참고문헌]

- [1] Internet of Things Architecture, <http://www.ietf.org/public>
- [2] D. Gessner, A. Olivereau, A. Salinas Segura, A. Serbanati, 'Trustworthy Infrastructure Services for a Secure and Privacy-respecting Internet of Things,' IEEE Conference on Trust, Security and Privacy, 2012.