사물인터넷(IoT) 플랫폼 보안

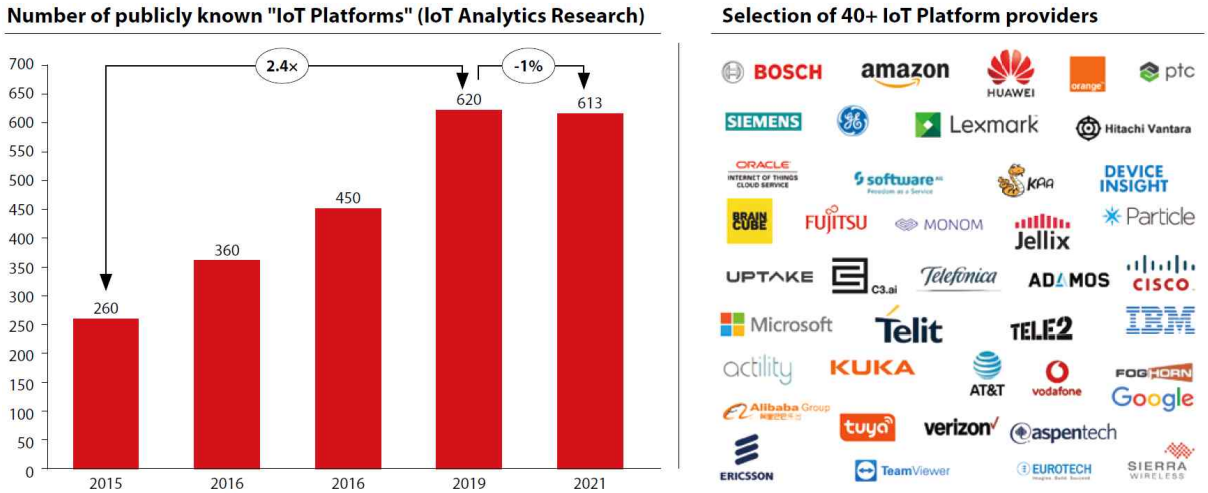
김영갑 세종대학교 정보보호학과 교수

1. 머리말

최근 사물인터넷(Internet of Things; IoT) 기술은 스마트홈, 헬스케어, 스마트시티, 물류, 스마트카 등 다양한 영역에 적용되어 확장되고 있다. 국제 표준인 "ISO/IEC 20924:2021 – Internet of Things (IoT) - Vocabulary"에서 사물인터넷은 "물리적 세계와 가상 세계의 정보를 처리하는 서비스와 상호 연결된 개체 및 정보 자원의 인프라"로 정의한다. 즉, 사물인터넷은 네트워크, 장치, 플랫폼의 종류에 관계 없이 인간의 개입을 최소화하면서 사물, 서비스, 인간 사이의 끊임없는 서비스를 제공하기 위한 초연결성[1] 기술로 정의될 수 있다.

사물인터넷 관련 기술, 표준, 프로젝트는 다양하게 지속적으로 개발되고 있다. 특히 사물인터넷 플랫폼은 다양한 도메인에서 수많은 센서, 액세스 포인트, 네트워크 간의 연결을 지원하고 사용자에게 서비스를 제공하는 중요 구성 요소로, 사물인터넷 전문 시장조사기관인 IoT Analytics에 의하면, [그림 1]과 같이 사물인터넷 플랫폼이 2017년 450개에서 2019년 620개 이상으로 증가하였으며, 2021년 이후에는 급격한 증가는 멈췄지만 600개 이상이 서비스를 제공하고 있다고 발표하였다. 대표적으로 AllSeen Alliance AllJoyn, Apple HomeKit, oneM2M, FIWARE, Google Cloud IoT, GS1 Oliot, IBM Watson IoT, Microsoft Azure, OCF IoTivity 등이 있다.

Number of publicly known "IoT Platforms" (2015–2021)



Source: IoT Analytics Research 2021; Note: IoT Analytics' definition of an IoT Platform has shifted slightly over time. Condition for republishing: Source citation with link to original post and company website; Non-commercial purposes only

[그림 1] 연도별 사물인터넷 플랫폼 수 (2015~2021) [3]

1) IoT 플랫폼/네트워크/단말 종류에 관계없이 인터넷으로 연결된 모든 사물이 사람의 직접적인 개입이나 지시 없이, 센서, 소프트웨어, 통신기능으로 네트워킹, 정보처리, 센싱 할 수 있는 사물 공간 환경

다만, 세계 3대 경영컨설팅 회사인 베인 앤드컴퍼니(Bain & Company, Inc)의 2018년도 사물인터넷의 가능성을 분석한 보고서의 내용에 따르면, 사물인터넷을 적용하는데 가장 방해가 되는 것으로 '보안' 요소를 지적하였다. 또한, 현재의 대부분 사물인터넷 플랫폼은 단일 플랫폼 내의 보안, 즉, 해당 사물인터넷 플랫폼에서 제공하는 서비스 및 해당 플랫폼에 접속된 장치에 대한 간단한 보안 기능만을 제공하고 있다. 즉, 다양한 사물인터넷 플랫폼이 개발되고 있지만 각 사물인터넷 플랫폼의 보안 구조 및 기능의 다양성과 이질성으로 인한 상호운용성 문제는 사물인터넷의 근본적 목표인 초연결성을 제한한다. 이에, 본 원고에서는 사물인터넷 플랫폼의 특성과 이에 따른 보안 요구사항을 살펴보고, 국제 표준으로 잘 알려진 사물인터넷 플랫폼들의 보안 구조와 기능들을 살펴보고자 한다.

2. 사물인터넷 플랫폼 특성 및 보안 요구사항

보안 요구사항은 안전한 서비스/시스템 구현을 위해 중요한 요소임에도 불구하고, 대부분은 서비스/시스템 개발 완료 후 보안 요구사항을 파악, 이를 만족하는 보안 솔루션 도입을 통해 개발되는 것이 일반적이다. 하지만, 이러한 구현은 서비스/시스템이 개발 초기부터 다양한 보안 취약점을 갖고 개발될 수 있을뿐더러, 향후 새로운 보안 요구사항 개발을 위해 보다 많은 비용이 소비될 수 있다. 이에 서비스/시스템 개발 초기 단계(즉, 요구사항 분석 단계)부터 보안 요구사항을 면밀히 분석해야 하며, 이를 서비스/시스템 설계, 구현, 테스팅, 배치 단계 등에 반영해야 한다.

앞서 언급한 바와 같이, 사물인터넷 플랫폼은 다양한 도메인에서 수많은 센서, 액세스 포인트, 네트워크 간의 연결을 지원하고 사용자에게 서비스를 제공하는 중요한 요소이다. 그러나, 사물인터넷 플랫폼이 서비스를 제공하는 과정에서 다양한 보안 이슈가 발생할 수 있으므로, 특히 사물인터넷의 특성들을 고려한 보안 요구사항을 충분히 고려해야 한다. 본 원고에서는 사물인터넷 특성 중에서 이종성(heterogeneity), 동적환경(dynamic environment), 자원제약성(resource constraint)에 초점을 두고, 이를 기반으로 보안 요구사항인 '보안 상호운용성'(interoperable security), '신뢰(trust)', '보안서비스 경량화(lightweight security service)'에 대해 강조하고자 한다.

2.1 이종성

이종성은 사물인터넷 장치의 종류 및 성능, 네트워크 프로토콜, 사물인터넷 플랫폼, 각종 정책 등의 다양성을 의미한다. 특히, 다양한 사물인터넷 플랫폼이 개발되고 있지만 각 사물인터넷 플랫폼의 기반 기술, 통신 프로토콜, 보안 정책 등이 상이하여 이기종 사물인터넷 플랫폼 간에 원하는 정보나 서비스를 교환하거나 사용하기에 많은 제한이 있다. 따라서, 사물인터넷 플랫폼은 이러한 이종성을 해결하기 위해 상호운용성(interoperability)을 보장해야 한다. 상호운용성을 보장하기 위해 일부 사물인터넷 플랫폼에서는 이기종 사물인터넷 플랫폼과의 상호운용 기술 및 방법을 개발하고 표준으로서 제안하고 있으나, 대부분이 자원(서비스, 데이터 등)의 상호운용에 초점이 맞추져 있다. 이에 안전한 사물인터넷 환경 구현을 위해서는 이기종 간의 상호운용 보안 기술에 대해서 고려해야 한다. 특히, 사물인터넷이 처음 소개(1999년)된 지 20여 년이 지났지만, 각 사물인터넷 플랫폼마다 독자적인 보안아키텍처, 보안정책 운영으로 보안 상호운

용문제를 해결하기까지는 많은 시간이 소요될 것으로 생각된다. 하지만, 안전하고 진정한 초연결 사물인터넷 환경을 만들기 위해서는 가장 중요한 보안 요구사항임을 결코 잊어서는 안된다.

2.2 동적환경

사물인터넷 플랫폼에는 다양한 사물인터넷 장치들이 연결되었다가 연결이 해제되는 등의 변화가 시시각각 이뤄진다. 이와 같이, 사물인터넷 플랫폼은 동적 특성을 가지며 이러한 동적환경에 맞춰 적절한 신뢰 관계를 성립 및 해제할 수 있어야 한다. 특히, 여러 사용자나 장치가 사물인터넷 플랫폼을 신뢰할 수 있도록 신뢰를 명확하게 정의하고 보안을 위해 신뢰를 추정하거나 평가하는 방법을 고려해야 한다. 또한, 신뢰를 기반으로 접근제어를 수행하는 과정에서 동적 환경 특성에 따라 접근제어 정책은 유연하게 확장될 수 있어야 한다.

2.3 자원제약성

사물인터넷에서 사용되는 대부분의 센서(sensor) 및 액추에이터(actuator)는 하드웨어 성능이 제한적이므로 사물인터넷 플랫폼은 이러한 장치들의 저사양 특성을 고려해야 한다. 다수의 사물인터넷 플랫폼에서는 이러한 특성으로 인해 MQTT(message queuing telemetry transport) 및 CoAP(constrained application protocol)과 같은 경량 통신 프로토콜을 사용하여 통신하고 있다. 또한, 사물인터넷 플랫폼은 통신과 함께 보안 서비스에 대해서도 경량화가 필요하다. 특히, 사물인터넷 장치의 저사양 특성으로 인해 플랫폼은 강력하고 성능 좋은 보안 서비스를 적용하기에 제한이 있다. 따라서 사물인터넷 플랫폼은 경량화된 인증(authentication)과 인가(authorization) 프레임워크 같은 보안 서비스를 제공해야 하며, 클라우드 기반 사물인터넷 플랫폼의 경우에는 클라우드에 보안 프로세스를위임하여 사물인터넷 장치에 성능 부담을 줄이는 것에 대한 고려가 필요하다.

3. 사물인터넷 플랫폼 보안을 위한 국제 표준화 기구 문서

본 절에서는 국제 표준화 기관에서 발간한 사물인터넷 관련 백서 및 지침을 통해 사물인터넷 플랫폼이 갖춰야 하는 보안 요구사항 및 기능들에 대해 살펴보고자 한다.

3.1 White Paper on 2022 Global Security

국제 표준인 ioXt Alliance 와 RCG CG(research center for global cyberspace governance)가 발표한 White Paper on 2022 Global Security는 사물인터넷의 발전과 수요의 증가에 따른 사물인터넷 보안을 다루고 있다. 본 백서에서는 사물인터넷 플랫폼 보안 예시와 함께 사물인터넷 플랫폼 측면에서 고려할 수 있는 사물인터넷 보안 고려사항들이 제시되었다. 예를 들어, 보안에 과소 또는 과대 투자를 피하기 위해 사물인터넷 장치에 요구되는 보안 수준을 식별하는 것, 공격자는 사물인터넷 장치의 가장 취약한 부분을 공격하려고 하기 때문에 사물인터넷 장치의 생명 주기 전반에 걸쳐 보안을 제공하는 것, 사물인터넷 장치마다 자체 보안 기준을 적용하면 각 사물인터넷 장치를 이해하고 신뢰하기 어려워지며 공격에 취약해지기 때문에 모든 사물인터넷 장치에 일관된 보안 기준을 적용하는 것 등이 제시되었다.

3.2 Guidance for Securing IoT Using TCG Technology Reference Document

하드웨어 기반의 신뢰 컴퓨팅 및 보안 기술 표준화 기구인 TCG(Trusted Computing Group)는 일반적인 사물인터넷 보안 사용사례를 설명하고 이러한 사용사례에 TCG 기술을 적용하기 위한 지침으로 Guidance for Securing IoT Using TCG Technology을 제공한다. 이 지침에서는 <표 1>과 같이 사물인터넷 플랫폼이 제공해야 하는 보안 기능을 설명하였으며, 각 보안 기능을 제공할 수 있는 TCG의 기술들을 제시하였다. 예를 들어, 공격자가 가장할 수 있는 장치 식별자인 GUID(globally unique identifier) 대신 암호화된 장치 식별자를 제공하고, 하드웨어 공격으로부터 키 보호 기능을 제공하는 TPM(trusted platform module), 악성 소프트웨어로부터 사물인터넷 장치를 보호하기 위해 펌웨어 및 운영체제가 사물인터넷 장치의 상태 일부 또는 전체 쓰기를 방지할 수 있는 로직을 포함하는 TCG SED(self-encrypting drive), 버전 정보를 포함한 특정 장치에서 실행 중인 소프트웨어 또는 펌웨어를 확인하는 표준화된 방법을 제공하는 TNC(trusted network communications) 표준 등이 있다.

<표 1> 사물인터넷 플랫폼에서 지원해야 하는 보안 기능

번호	항목
1	장치 식별자 설정 및 보호(Establishing and Protecting Device Identity)
2	악성소프트웨어 감염에 대한 보호(Protection Against Malware Infection)
3	하드웨어 변조에 대한 보호(Protecting Against Hardware Tampering)
4	유휴 데이터의 무결성, 기밀성, 가용성(Confidentiality, Integrity, and Availability of Data at Rest)
5	장치의 재판매 또는 폐기(Reselling or Decommissioning a Device)
6	암호 프로토콜 요구사항 충족(Meeting Cryptographic Protocol Requirements)
7	다양한 프로비저닝 모델 지원(Supporting Multiple Models of Provisioning)
8	감사 로그 유지(Maintaining Audit Logs)
9	원격 관리(Remote Manageability)
10	레거시 하드웨어 보호(Securing Legacy Hardware)

4. 국제 표준 기반 사물인터넷 플랫폼 및 보안 구조

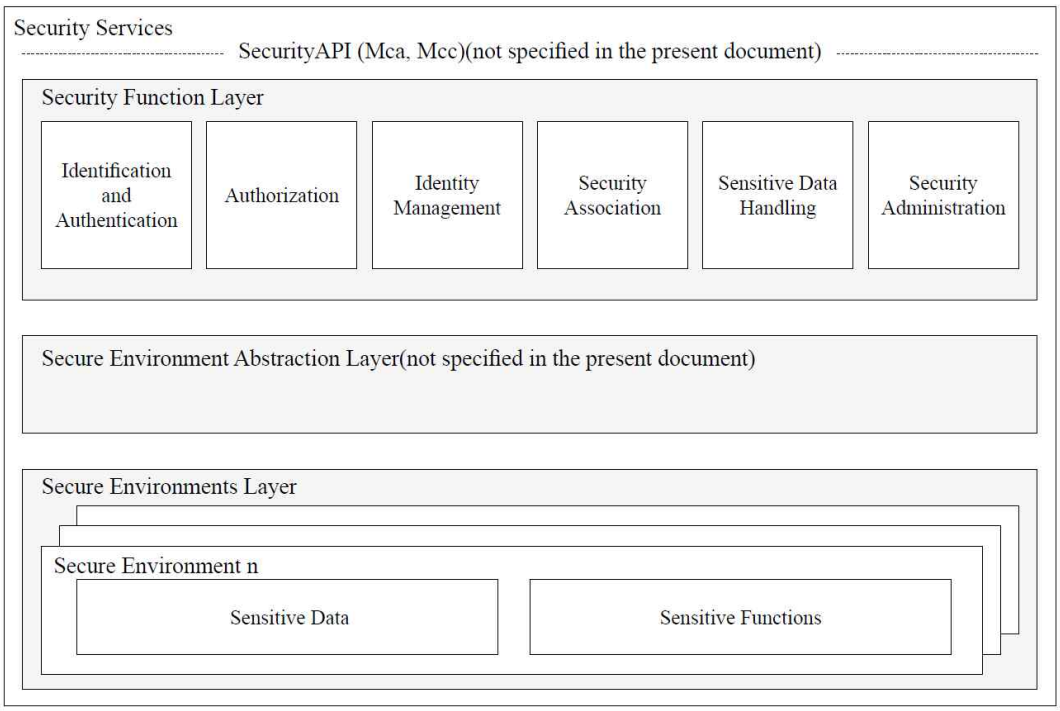
정보통신기술 분야에서 국제적으로 다양한 활동을 수행하는 조직 및 기구들이 사물인터넷 시장을 선점하기 위해서 AllSeen Alliance AllJoyn, Apple HomeKit, oneM2M, FIWARE, Google Cloud IoT, GS1 Oliot, IBM Watson IoT, Microsoft Azure, OCF IoTivity 등과 같은 사물인터넷 플랫폼을 개발하고 있다. 본 원고에서는 이러한 사물인터넷 플랫폼 중에서 국제 표준화 기구에서 개발 중인 oneM2M, FIWARE, OCF IoTivity 플랫폼 중심으로 각 플랫폼의 보안 구조 및 특징에 대해 살펴보고자 한다.

4.1 oneM2M

oneM2M은 수많은 M2M(machine to machine) 장치를 연결하기 위해 다양한 시스템에 내장될 수 있는 표준 M2M 서비스 계층 기술 규격서 및 사물인터넷 플랫폼을 개발하는 국제 표준화

기구이다.

oneM2M의 보안 구조는 [그림 2]와 같이 보안 기능 계층(security functions layer), 보안 환경 추상화 계층(secure environment abstraction layer), 보안 환경 계층(secure environments layer)으로 구성된다. 보안 기능 계층은 식별 및 인증, 인가, 식별자 관리, 민감 데이터 관리, 보안 관리 기능을 제공한다. 보안 환경 추상화 계층은 데이터 암호화/복호화, 서명 생성/검증, 보안 자격증명 읽기/쓰기 등과 같은 다양한 보안 기능을 제공하며, 보안 환경 계층은 중요한 데이터 스토리지 및 중요한 기능 실행에 대한 적절한 보호를 제공하는 다양한 보안 서비스를 제공하는 하나 이상의 보안 환경이 포함된 계층이다. 특히, oneM2M은 CSE(common service entity)와 AE(application entity)와 같은 구성 노드가 제대로 신뢰할 수 있는 자격 증명을 가지는지 검증한다. 인증서 기반 인증 메커니즘을 사용하는 경우에는 디지털 서명을 확인하기 위한 인증 기능을 사용하고, 대칭키 기반 인증 메커니즘을 사용하는 경우에는 메시지 무결성 코드를 확인하기 위한 인증 기능을 사용한다. 또한, 프로비저닝된 액세스 제어 정책 및 할당된 역할에 따라 사용자에게 권한 부여를 제공하며, 액세스 제어 목록 및 역할 기반 액세스 제어와 같은 다양한 인증 메커니즘을 지원한다.

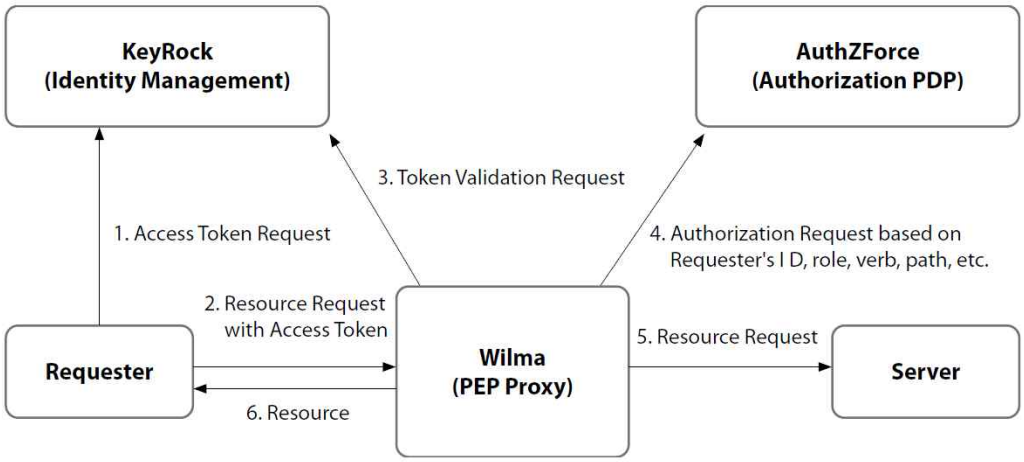


[그림 2] oneM2M의 보안 구조 [7]

4.2 FIWARE

FIWARE는 NGSI(next generation service interfaces) 표준 기반으로 오픈소스 플랫폼으로, 유럽 내 미래 인터넷 공공-민간 파트너십(FI-PPP)에 의해 개발된 지능형 솔루션(예를 들어, 스마트 시티, 스마트 농식품, 스마트 에너지 및 스마트 산업)을 가속하기 위해 개발된 플랫폼이다. FIWARE에서는 [그림 3]과 같이 신원 관리(예를 들어, 역할 및 권한 할당)를 통해 애플리케이션 내 사용자를 관리하는 보안 구조를 제

공한다. 특히, FIWARE 보안 아키텍처는 OAuth 2.0을 기반으로 역할기반 접근제어를 포함한 다양한 접근제어 모델을 사용할 수 있도록 Keyrock, AuthzForce, Wilma라는 세 가지 컴포넌트를 제공한다. Keyrock은 플랫폼에 등록된 사용자, 조직, 애플리케이션의 신원을 관리하는 컴포넌트로서 등록된 사용자 자격증명을 토대로 사용자 인증을 수행하고 OAuth 인가 방식에 따라 사용자에게 액세스 토큰을 제공한다. 특히, 사용자에 대해서 이중 인증(two-factor authentication)을 수행할 수 있으며 OAuth 표준에서 제공하고 있는 4개의 인가 방식을 모두 지원한다. AuthzForce는 FIWARE에서 PAP(policy admin point)와 PDP(policy decision point)를 수행하는 컴포넌트로, 접근제어 정책을 토대로 사용자가 자원에 접근할 수 있는 지를 결정하여 Wilma에 인가 결과를 전달하는 역할을 한다. 마지막으로, Wilma는 PEP(policy enforce point)로 PEP proxy라고도 불리며 자원을 보호하는 엔드포인트(endpoint) 역할을 수행한다.



[그림 3] FIWARE의 보안 구조 [8]

4.3 OCF IoTivity

OCF는 사물인터넷 산업에서 상호운용성 지침, 표준 및 인증 시스템을 제공하는 국제 기구이며, 사물인터넷 장치 간에 쉽고 안전한 통신을 제공하기 위해 IoTivity 플랫폼을 개발 중에 있다. OCF 표준에 따르면, 보안 목표는 자원 보호 및 이를 지원하는 하드웨어 및 소프트웨어를 보호하는 것이다. 이에 따라서, OCF 보안 아키텍처는 장치 간 상호 작용 중에 보안 메커니즘 및 정책을 준수하여 자원에 대한 클라이언트 액세스 권한을 장치에 제공한다. 특히, IoTivity 보안 구조인 [그림 4]에서 SRM(security resource manager)은 보안을 제공하는데 중요한 역할로서 플랫폼의 안전한 실행을 위해 모듈식으로 설계되며, RM(resource manager), PE(policy engine), PSI(persistent storage interface)로 구성된다. IoTivity의 보안 구조에서 액세스 제어 정책은 ACE(access control entry)로 ACL(access control list)에 저장되며 자원에 대한 액세스는 연결된 ACE를 사용하여 제어된다. 액세스 제어 메커니즘에는 SBAC(subject-based access control), RBAC(role-based access control) 및 와일드카드 기반 액세스 제어가 포함된다. SBAC은 클라이언트의 ID를 자원에 대해 정의된 정책의 주체와 일치시키고 RBAC은 자원에 대한 정책에 포함된 역할 식별자를 클라이언트와 연결된 역할 식별자와 일치시킨다. 마지막으로 와일

드카드 기반 액세스 제어는 ACE가 연결 유형과 일치하는 자원에 액세스하는 데 사용된다.

5. 맺음말

사물인터넷 기술이 발전함에 따라 다양한 도메인에 접목되어 사용자와 서비스 간의 연결을 제공하는 사물인터넷 플랫폼 관련 기술 수요가 늘어났지만, 사물인터넷 플랫폼의 독자적인 개발과 이를 통합할 수 있는 표준의 적용이 이뤄지지 않고 있다. 이는 네트워크, 장치, 플랫폼의 종류와 관계없이 인간의 개입을 최소화하면서 사물, 서비스, 인간 사이의 끊김 없는 서비스를 제공하는 사물인터넷의 목표에 제한이 되며, 진정한 의미에서의 초연결 사회를 기대하기 어렵다. 다시 말해, 다양한 사물인터넷 플랫폼 간의 자원 요청 및 공유와 같은 상호운용성이 중요시 되어야 하며, 사물인터넷 플랫폼 종류와 상관없이 지속적인 서비스를 사용자에게 제공할 수 있는 안전하고 진정한 사물인터넷 환경을 구축하기 위한 방안 및 기술들이 고려되어야 한다.
본 원고에서는 사물인터넷 플랫폼의 특성과 사물인터넷 플랫폼이 가져야 하는 보안 요구사항에 대해 살펴보았다. 특히, 사물인터넷의 특징인 이종성, 동적환경, 자원제약성 측면에서 사물인터넷 플랫폼이 갖추어야 할 보안 요구사항을 살펴보았다. 또한, 사물인터넷 관련 국제 표준화 기관의 백서 및 지침 문서를 통해, 사물인터넷 플랫폼이 갖추어야 할 보안 요구사항 및 보안 기능을 식별하였고, 대표적 국제 표준화 기구에서 개발 중인 oneM2M, FIWARE, IoTivity 플랫폼의 보안구조와 보안 기능에 대해 살펴보았다.
사물인터넷 환경에서 사물인터넷 플랫폼은 다양한 사물(things) 간 연결을 지원하고 서비스를 제공하는 중요한 요소이다. 아직까지는 각 플랫폼 중심의 독자적인 서비스 및 보안 솔루션 개발에 치중하고 있고, 이기종 플랫폼 간 상호운용 기술에 대한 기술 및 솔루션은 미흡한 실정이다. 이에, 안전하고 초연결 사물인터넷 환경 구축을 위해서는 사물인터넷 플랫폼이 가지고 있는 특성에 기반한 보안 요구사항을 면밀히 검토해야 하고, 특히, 이기종 사물인터넷 플랫폼 간의 보안상호운용성 문제를 해결하기 위한 지속적인 연구가 필요하다.

※ 본 연구는 '정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구(No.2021R1A2C2012635) 결과의 일부 내용을 발췌하였으며, 관련 논문 및 표준문서의 참고 버전임.

[주요 용어 풀이]

- 사물인터넷 플랫폼(IoT Platform): 다양한 도메인에서 수많은 센서, 액세스 포인트, 네트워크 간의 연결을 지원하고 사용자에게 서비스를 제공하기 위한 미들웨어
- 상호운용성(Interoperability): 하나 혹은 그 이상의 시스템이나 애플리케이션들이 상호 정보를 교환하고 교환된 정보를 사용할 수 있도록 하는 기능으로서, 다른 종류 또는 다른 유형의 자원 간에 통신할 수 있고, 정보 교환이나 일련의 처리를 실행하는 것
- 보안 요구사항(Security Requirements): 보안 관련 계약, 표준, 명세 또는 다른 형식으로 제시된 문서에 적합하여 시스템이나 시스템 구성 요소가 갖추어져야 할 조건이나 능력

[참고문헌]
[1] 김영갑, 사물인터넷 보안 요구사항, 주간기술동향 1793호, 2017
[2] ISO/IEC 20924:2021, 2021, Information technology - Internet of Things (IoT) - Vocabulary.
[3] WEGNER, P, IoT Analytics, "IoT Platform Companies Landscape 2021/2022: Market consolidation has started", https://iot-analytics.com/iot-platform-companies-landscape/
[4] ioXt, White Paper on 2022, "Report on 2022 Global IoT Security", 2022.
[5] Trusted Computing Group, "Guidance for Securing IoT Using TCG Technology. Version 1.0 Revision 21", 2015.
[5] ioXt, White Paper on 2022, "Report on 2022 Global IoT Security", 2022.
[6] oneM2M, https://www.onem2m.org/harmonization-m2m
[7] oneM2M Security, "TS-0003 V. 3.10.2 oneM2M - Security Solutions", oneM2M, 2019.
[8] 오세라, 김영갑, "사물인터넷 보안 인터워킹에 대한 연구", 2017년 추계학술발표대회논문집, 24권, 2호, pp.1283-1286, 2017
[9] FIWARE, https://www.fiware.org
[10] FIWARE, "Identity Management", https://ngsi-ld-tutorials.readthedocs.io/en/latest/identity-management.html/
[11] IoTivity, https://iotivity.org
[12] Open Connectivity Foundation, "OCF Security Specification VERSION 2.2.6", https://openconnectivity.org/developer/specifications/

※ 출처: TTA 저널 제206호