Journal of the Korea Convergence Society
Vol. 8. No. 10, pp.61-66, 2017 https://doi.org/10.15207/JKCS.2017.8.10.061

# CC 기반의 안전한 IoT 시스템 설계 방안

김주훈[1], 정현미[2], 조한진[3*]
[1]한국정보통신기술협회, [2]한국과학기술정보연구원, [3]극동대학교

# Design Plan of Secure IoT System based Common Criteria

Ju-Hun Kim[1], Hyun-Mi Jung[2], Han-Jin Cho[3*]
[1]Management & Planning Division, TTA
[2]Dept. of Supercomputer System Development, KISTI
[3]Dept. of Energy IT Engineering, Far East University

**요 약** 최근 IoT기술은 '언제, 어디서나, 편리하게' 라는 키워드와 함께 급속도로 발전하고 있다. 이와 더불어 IoT 시스템에 대한 보안이슈가 폭발적으로 증가하고 있으며 그에 대한 피해도 커지는 상황이다. 이에 본 논문에서는 IoT 시스템 보안 요구사항을 정의하는 표준화와 보안기술개발 현황을 파악하고 ICT에서 국제적으로 통용되는 CC평가를 이용하여 안전하게 IoT 시스템을 개발하는 방안을 제시한다. 이를 위하여 우선 IoT 시스템과 서비스 측면의 보안목적을 분석 하였다. 향후 이를 토대로 보안기능요구사항을 설계하고 대응관계 통하여 보안목적의 이론적 근거가 증명할 수 있으며 IoT 시스템에 대한 보호프로파일설계가 가능하다. 이는 관리자, 개발자, 사용자 측면의 보안요구집합을 참조할 수단으로 사용되므로 본 논문에서 제시하고자하는 개발 방법론에 대한 충분한 근거가 된다.

• 주제어 : IoT 시스템 보안, IoT 시스템 보안요구사항, CC평가, IoT 시스템 보안 표준화, PP

**Abstract** Recently, IoT technology is rapidly developing with the keyword "Anytime, Anywhere, Convenient". In addition, security problems in IoT systems are exploding and the damage is increasing as well. In this paper, we propose a method to develop IoT system safely by using internationally recognized CC evaluation in ICT by identifying the standardization and security technology development status defining IoT system security requirements. For this purpose, IoT system and service security aspects are analyzed. Based on this, it is possible to design the security functional requirements and to demonstrate the rationale of the security objective through the correspondence relation, and it is possible to design the protection profile for the IoT system. This is a sufficient basis for the development methodology to be presented in this paper because it is used as a means of referring to the set of security requirements of administrators, developers, and users.

• Key Words : IoT, CC, Secure System, IoT Security functional Requirement, Protection Profile

## 1. 서론

IoT 가 발전하면서 기술의 기반이 되는 ICT 기반측면뿐만 아니라, 연결된 사물들에 대한 보안취약성 이슈가 폭발적으로 증가하고 있다. IoT의 발전은 ICT 인프라 측

*Corresponding Author : 조한진(hanjincho@hotmail.com)
Received August 18, 2017 Revised September 29, 2017
Accepted October 20, 2017 Published October 28, 2017

면에서 가상의 업무를 지원하는 것에서 물리환경으로의 확대라고 볼 수 있다.

이러한 이유로 다양한 측면으로의 보안 위협이 대두되고 있으며 피해도 그 예상치를 가늠할 수 없는 상황이다. 예를 들어 실생활과 직접적 연관이 있는 커넥티드 카, 스마트 홈 등의 디바이스에 대한 다양한 해킹 시나리오가 가능하다. 특히 전력, 가스, 상하수도 등은 스마트 홈 시스템이기도 하지만 국가기반시설인 스카다(SCADA: Supervisory Control and Data Acquisition)시스템이기도 하다[1]. 이런 중요시설에 대한 해킹 이슈도 확산되고 있어 해킹이 실현되면 그 피해는 경제적 손실뿐만 아니라 국가적 위기로까지 예상되고 있다. 때문에 IoT 보안 대책을 연구하고 개발하는 것은 반드시 해야 할 사항이다.

그러나 대부분의 ICT보안 사고를 살펴보면 표준화되지 않은 보안 적용, 복잡하게 구성된 보안체계 및 비체계화된 보안 모니터링 등의 문제를 가지고 있으며 더군다나 다양한 ICT가 적용된 IoT 에 대하여 완벽한 보안 체계를 만드는 것은 쉬운 일이 아니다. 더불어 IoT의 비약적인 발전 속도가 보안에 대한 이슈가 증가의 한 요인으로 작용하고 있다.

이러한 이유로 IoT 디바이스를 비롯한 서비스에 대한 보안 체계 등에 대한 표준화 가이드 등이 반드시 마련되어야 하며 본 논문에서는 사용자, 개발자, 서비스제공자 등 서비스모델에서의 각 단말의 최종 사용자에 대한 보안요구의 집합을 참조할 수단을 공유수단인 공통평가기준(CC: Common Criteria)을 통한 안전한 IoT 시스템 설계방안을 제시한다[2,3,4,5].

## 2. 관련연구

### 2.1 IoT 정의

2000년대 초반 유비쿼터스(Ubiquitous), M2M (Machine to Machine) 등 즉, 언제, 어디서나, 편리하게, 사물 간 통신, 사람 사물 간 통신 등의 키워드들과 함께 ICT가 급속도로 발전하기 시작하였다[6].

특히 유비쿼터스는 "어디에나 있음"을 의미하며 라틴어 'ubique'를 어원으로 하는 영어의 형용사로 '동시에 어디에나 존재하는, 편재하는'이라는 사전적 의미를 가지고 있다. 따라서 이 기술은 현재의 IoT의 "언제, 어디서나, 편리하게" 라는 키워드와 무관하지 않다[7]. 즉, 시간과 장소에 구애받지 않고 언제나 정보통신망에 접속하여 다양한 정보통신서비스를 활용할 수 있는 환경을 의미하는 차원으로 유비쿼터스는 IoT의 시작점이라고 할 수 있다.

IoT의 개념은 연결의 주체, 능동성, 정도 및 방식의 4가지 관점에서 다음과 같이 분류가 가능하다[8,9].

#### 1) 연결의 주체

기존 M2M의 경우 '머신' 중심의 연결 의미가 크지만 IoT는 '환경' 중심의 연결을 의미한다. IoT는 사물과 사물간의 연결보다는 사람과 사물 주변의 환경이 연결에 대한 주체가 됨으로써 확대된다는 것을 의미한다.

#### 2) 연결의 능동성

IoT는 사물이 정보를 수집하고 가공하여 인간에게 수동적으로 전달하는 것뿐만 아니라 사물 학습을 기반의 정보 생성, 가공 및 공유가 가능하고 인간과의 상호작용을 하는 등 지능정보 생성이 가능하다.

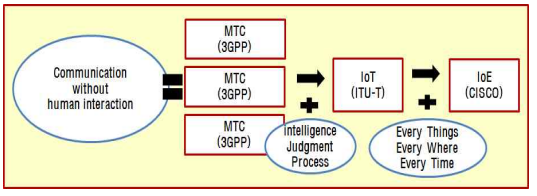
#### 3) 연결의 정도

IoT의 연결의 정도는 단지 통신하는 것뿐만 아니라 사물이 사물 및 인간의 주변 환경을 인지하고 정보를 생성·공유함으로써 상호 작용까지 가능하다.

#### 4) 연결 방식

IoT은 단지 유·무선 네트워크를 사용하는 개념에서 벗어나 '공공 또는 민간 IP를 사용하는 것'이라고 보기도 한다. 한편으로는 유 무선통신 IoT으로 변모한다고 보는 관점도 존재한다.

다음 [Fig. 1]에서는 주요 기관들에서 IoT 관련 용어를 도식화 한 것이다[8,9,10,11].




[Fig. 1] IoT

### 2.2 IoT 보안 동향

기하급수적으로 증가하는 IoT 보안 이슈 해결을 위하여 ICT 보안기술을 이용한 IoT 서비스를 출시하거나

IoT만을 위한 보안기술을 개발하는 추세이다. 이에 본 절에서는 IoT 시스템 보안 요구사항을 정의하는 표준화와 보안기술개발 현황을 살펴본다[12].

#### 2.2.1 IoT의 보안요구사항을 정의하는 표준화 활동

IoT보안 요구사항은 국제적으로 ITU-T, IETF 등 일부 표준화 단체를 중심으로 논의되고 있으며 ITU-T는 IoT 표준 참조모델을 통하여 디바이스, 어플리케이션, 네트워크 등에서 고려되어야 할 보안 요구사항들을 키워드로 제시하고 있다. IETF의 CoRE 워킹그룹에서는 IP기반의 IoT 서비스들을 위험수준에 따라 분류하고, 각각의 분류 체계별로 고려되어야할 보안 요구사항들을 논의 중이다.또한 전기·전자, 통신, 인터넷 등 다양한 분야의 표준화 단체는 IoT 환경에 적합한 경량 인증・암호화 기술에 대한 연구 추진하고 있다.

우선 IETF는 저전력·경량 기기를 위한 IoT 통신 프로토콜(CoAP) 및 보안 구조·모델 정의하고 있으며 ITU-T는 앞서 말한 것처럼 IoT 보안 요구사항 및 경량 인증·암호화 기술을 IoT 통신 프로토콜(CoAP, MQTT 등)에 적용하는 방안 논의 중이다.

ISO는 IoT에 적용 가능한 경량암호 알고리즘(HIGHT, PRESENT)을 표준화하고 있으며 3GPP의 SA3 그룹에서 이동통신 기반의 기기 간 안전한 통신을 위한 인증·암호화 표준화 작업을 진행하고 있다.

#### 2.2.2 IoT에 특화된 보안기술을 개발 현황

Verizon는 클라우드 기반의 IoT 기기 식별·인증, 통신 데이터 보호를 위한 보안솔루션 MCS(Managed Certificate Services) 개발하였으며, Cisco는 IoE 환경에 필요한 인증, 권한관리 및 접근제어, 강제화 된 네트워크 정책 등으로 구성된 보안 프레임워크 제안하였다. WindRiver는 모듈단위의 재구성이 가능한 IoT 전용 보안 운영체제인 VxWorks 7를 개발 14년도에 개발하였다.

### 2.3 공통평가기준

앞서 언급한 것처럼 본 논문에서는 CC를 이용하여 안전한 IoT 시스템을 설계하고자 한다. CC는 ICT 제품의 보안 기능성 평가 과정에서 타겟이 되는 대상의(TOE: Targer of Evaluation) 보증수단에 대한 공통요구사항을 제시함으로써, 독립적으로 수행된 보안성 평가의 결과를 비교가능하게 한다. 또한 CC에서의 보호프로파일(PP: Protection Profile)은 사용자, 관리자, 개발자 영역 등 모든 그룹의 보안요구의 집합을 정의한 문서이므로 CC는 IT 제품의 전체 혹은 그 일부 가능을 평가 할 때 사용된다. 즉 보안 평가 과정은 TOE의 보안 기능성과 이에 적용된 보증수단이 요구사항들을 만족하는지에 대한 신뢰도를 확인하는 것이며 평가결과는 최종 사용자가 TOE의 보안 요구를 충족시키는지 를 결정 가능한 기준이 된다. 따라서 CC는 보안 기능성이 있는 ICT 제품 등의 개발, 평가에 대한 지침으로 활용가능하다[2,3,4].

## 3. 안전한 IoT 시스템 개발 방안

본 논문에서 제시하고자 하는 CC기반의 안전한 IoT 시스템을 개발하기 위하여 보안목적분석과 보안기능요구사항 설계가 선행 되어야 하며 이들의 대응관계 통하여 보안목적의 이론적 근거가 증명가능하다[10-12].

### 3.1 IoT 시스템 보안 목적 정의

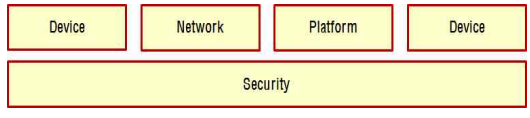
본 절에서는 안전한 IoT 시스템 개발을 위해서 시스템아키텍처, 디바이스 영역, 네트워크영역, 플랫폼 영역 및 서비스 아키텍처에 보안목적 정의한다.

#### 3.1.1 IoT 시스템 아키텍처 보안 목적

IoT는 사물기반이므로 임베디드 아키텍처와 매우 유사하게 보이지만, 사물이 인터넷에 연결되어 다양한 정보를 수집하는 관점에서 보면 임베디드 아키텍처와 차이가 있다. [Fig. 2]는 IoT 시스템 아키텍처 이다.

이를 기반으로 IoT 아키텍처의 보안목적을 다음 5가지로 정의 가능하다[13].

1) 다양한 디바이스를 지원 가능한 확장성 보장
2) 사람의 제어가 불필요한 자율성 보장
3) 장애를 극복하고 기능을 지속적인 수행이 가능한 탄력성 보장
4) 장시간 사용에도 견딜 수 있는 내구성 보장
5) 사물과 사물 또는 사물과 사람간의 원활한 커뮤니케이션이 가능한 접속성 보장




[Fig. 2] System architecture for IoT

다른 측면에서 보면 IoT는 ICT 기술과 각각의 산업의 서비스 영역의 유기적 결합으로 새로운 서비스를 제공한다. 따라서 안전한 IoT 시스템 개발을 위해서는 다양한 IoT 요소 기술 및 서비스 영역에서의 보안목적을 최대한 수용 가능 하도록 개발 되어야 한다[14].

#### 3.1.2 IoT 디바이스 보안 목적

디바이스 영역은 서비스를 위한 데이터 생성, 서비스 요청에 따른 반응이 나타나는 영역이다. 이를 위하여 사물의 주변 환경의 정보를 전기적인 시그널로 바꿔주는 센서나 전기적인 시그널을 물리적인 변화로 바꿔주는 액추에이터 그리고 이러한 시그널들을 주고받기 위한 통신 모듈 등을 포함하게 된다[15].

#### 3.1.3 IoT 네트워크 보안 목적

IoT 디바이스가 생성한 데이터들은 IoT 서비스 플랫폼으로 전달되어야 하며 이러한 역할을 담당 하는 것이 네트워크 이다. 네트워크 영역에는 통신 거리, 전송속도 및 통신 방식 등 서로 다른 특성을 가지고 있는 다양한 통신기술들이 존재 한다. 이 외에도 서비스 생성을 지원하는 기술, 데이터의 흐름 제어기술 등이 존재한다[16].

#### 3.1.4 IoT 플랫폼 보안목적

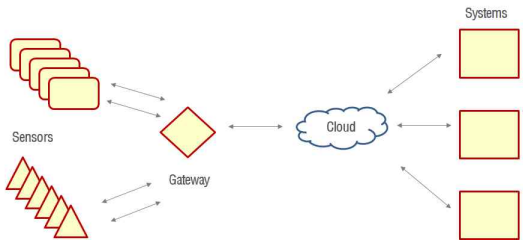
IoT 플랫폼이란 다양한 IoT 서비스 제공을 위하여 다양한 사용자 및 사물 간 중계자 역할을 하는 장치를 의미한다. 따라서 특별한 응용 서비스에 속해있지 않고 사물의 연결, 데이터의 수집·분석 및 지능형 서비스의 생성 등 서비스별 공통 서비스 기능을 수행한다.

#### 3.1.5 IoT 서비스 보안 목적

IoT 리소스/서비스 관리, 보안인증, 수집 데이터의 가공 및 처리 등은 IoT 서비스의 주요 기능이다. 이러한 서비스에는 지식정보(Semantics & Knowledge)형, 보안인증(Security & Privacy)형, 응용서비스(Application & Service) 형 등이 있다[17].

이들 맞춤 서비스, 빅데이터 기반으로 정보를 분석하고 예측된 정보 및 IoT와 소프트웨어의 인증과 연동 기능 등을 제공한다. 이런 내용을 기반으로 [Fig. 3]와 같은 IoT 서비스 아키텍처가 구성될 수 있다.

이에 네트워크 대역폭을 낮춰주고, 분석이 불필요한 데이터를 제거하며 과도한 데이터 수집을 줄이는 역할도




[Fig. 3] Service architecture for IoT

한다. 예를 들어 무선 네트워크 노드에서 수집된 정보가 게이트웨이에서 걸러져서 클라우드로 저장되고 빅데이터로 분석되어 사용자에게 필요한서비스 형태로 제공된다.

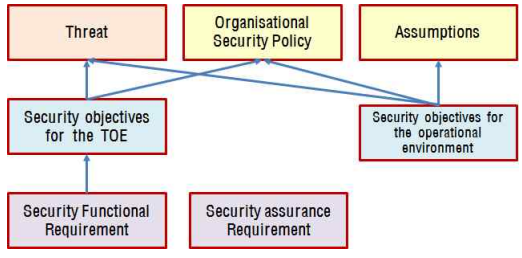
이를 토대로 서비스 별로 각자의 서비스 플랫폼을 가지게 된다. 서비스 플랫폼은 앞 단의 IoT 구성요소를 연결하는 역할과 데이터 기반 서비스를 제공하는 역할을 수행하게 되며 서비스 플랫폼을 표준형으로 구성한다면 초기 공수는 많이 들어갈 수 있으나 확장이 용이하다. 한편으로는 각 개별의 IoT 서비스를 독립적 모듈 형태로 제공가능하게 구성하면 IoT 서비스 아키텍처에 IoT 서비스를 쉽게 추가 가능하다.

### 3.2 안전한 IoT 시스템 개발 근거

앞에서 제시한 IoT 시스템의 보안 목적은 보안기능요구사항의 이론적 근거가 되며 보안기능요구사항은 다음을 입증한다.

- 각 TOE 보안목적은 적어도 하나의 TOE 보안기능요구사항에 의해서 다루어진다.
- 각 TOE 보안기능요구사항은 적어도 하나의 TOE 보안목적을 다룬다.

다음 [Fig. 4]은 보안문제 정의, 보안목적, 보안요구사항 간의 관계를 나타낸 것이다[1-3].




[Fig. 4] Relations between the security problem definition, the security objectives and the security requirements

따라서 보안목적의 이론적 근거는 명세한 보안목적이 적합하고, 보안 문제를 다루기에 충분하며, 과도하지 않고 반드시 필요한 것임을 입증한다.

## 4. 결론

결론적으로 IoT 보안에서의 미들웨어 인간과 사물 또 이기종 사물간의 통신이라는 특성과 멀티 디바이스 및 멀티 ICT의 결합이라는 측면에서 설계단계부터 고려되어야 한다. 그러나 IoT 미들웨어는 그 형태와 목적이 서로 상이한 이기종간의 하드웨어, 프로토콜 및 통신 등을 전 영역에 걸쳐서 다양한 형태로 존재하며. 그 역할에 따라 종류별로 달리 설계하더라도 공통적으로 보안을 강화할 수 있는 방안이 필요하다. 최근 IoT 통합미들웨어 등의 기술이 제안되고 있으나 이 또한 국제적으로 통용되고 있는 기준이 명확하지 않다. 이에 본 논문에서는 국제적으로 통용되는 기준인 CC평가를 적용한 IoT 미들웨어 설계 방법을 제시하였다. 향후 본 논문에서 제시된 방법론 적용을 위해서는 첫째 TOE를 정의하기 위한 IoT 시스템 모델링을 수행하고 TOE의 보안문제 정의, 보안목적 및 보안기능요구사항을 정의하고 그 상관관계를 나타냄으로서 개발에 대한 검증을 수행에 대한 연구를 지속해 나갈 예정이다. 본 연구를 토대로 IoT 미들웨어에 대한 보호프로파일설계(Protection Profile)가 가능하며 이는 관리자, 개발자, 사용자 측면의 보안요구의 집합을 참조할 수단을 공유하기 때문에 본 논문에서 제시하고자하는 개발 방법론에 대한 충분한 근거가 될 것이다.

## REFERENCES


[1] Computerworld, "Siemens: Stuxnet worm hit industrial systems", September 16, 2010.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, CCMB-2006-09-001,

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 2, CCMB-2007-09-002,

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 2, CCMB-2007-09-003,

[5] J. H. Kim, A Middleware Development Method for Internet of Things(IoT) Security, Master thesis of Far East University, 2017.

[6] Ashton, Kevin. "That 'Internet of Things' Thing."RFiD Journal, 22, pp 97-114, 2009.

[7] https://ko.wikipedia.org/wiki/전재

[8] Lee, Geo-Spatial Information System, Kumiseokwan Press, 2016.

[9] L. Atzori, A. lera, G. Moraito, "The Internet of Things: A survey", Computer Networks, vol 54, no. 15, pp. 2787-2805, Oct. 2010.

[10] KIET, Hyper Connected Society IoT Activation Plan 2014.

[11] http://cafe.naver.com/rapid7/2041

[12] http://www.lgcns.com/LGCNS.GHP.Main/Solution/IoTPlat form_En.

[13] NIPA, IoT Case Study - Architecture, 2016.

[14] http://blog.naver.com/human1500/220785377334.

[15] Mellado, Daniel, Eduardo Fernández-Medina, and Mario Piattini. "A common criteria based security requirements engineering process for the development of secure information systems." Computer standards & interfaces 29.2 (2007): 244-253.

[16] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "Siot: Giving a social structure to the internet of things." IEEE communications letters 15.11 (2011): 1193-1195.

[17] Babar, Sachin, et al. "Proposed security model and threat taxonomy for the Internet of Things (IoT)." Recent Trends in Network Security and Applications (2010): 420-429.

## 저자소개


김 주 훈(Ju-Hun Kim) [정회원]

- 2012년 2월 : 극동대학교 스마트모바일학과(공학사)
- 2017년 8월 : 극동대학교 스마트모바일학과(공학석사)
- 2013년 8월 ~ 현재 : 한국정보통신기술협회 근무중

<관심분야> : 사물인터넷, 정보보안, 클라우드 컴퓨팅

정 현 미(Hyun-Mi Jung) [정회원]

- 2014년 2월 : 한남대학교 컴퓨터공학전공(공학박사)
- 2012년 10월 ~ 현재 : 한국과학기술정보연구원 슈퍼컴퓨터시스템개발실 선임연구원

<관심분야> : HPC, HPC 보안, 클라우드 컴퓨팅

조 한 진(Han-Jin Cho) [종신회원]

- 2002년 8월 : 한남대학교 컴퓨터공학과(공학박사)
- 2002년 3월 ~ 현재 : 극동대학교 에너지IT공학과 교수

<관심분야> : 모바일 보안, IoT 보안, 융합 콘텐츠사물인터넷, 정보보안, 클라우드 컴퓨팅