IoT 보안 요구사항에 대한 고찰

김다빈
경희대학교
heartjigi@khu.ac.kr

김경모
시큐아이
doublekm@gmail.com

조진성
경희대학교
chojs@khu.ac.kr

Discussions on IoT Security Requirements

Dabin Kim
KyungHee University

KyeongMo Kim
SECUI

Jinsung Cho
KyungHee University

요 약

모든 사물(thing)에 정보통신기술(ICT)를 적용함으로써 창조된 개념인 IoT(Internet of Things)는 사물지능통신(M2M)을 기반으로 얻어지는 정보들을 분석하여 가치 있는 서비스를 창출한다. IoT의 대두로 인해 사물지능통신 장비들 운용이 증가하고, 이에 따라 다양한 요구사항이 발생하고 있다. 특히, 사물지능통신에서 발생하는 방대한 정보 기반의 악의적인 정보 가공 및 공급으로 인한 보안문제의 해결이 중요하게 대두되고 있다. 또한, IoT는 기존의 네트워크가 가지는 보안 특성을 그대로 계승하며, 사물지능통신으로 인한 추가적인 보안 이슈를 해결해야할 필요가 있다. 따라서 IoT의 현실화를 위해서는 사물지능통신을 통해 생기는 네트워크에서 생기는 보안문제와 기존 네트워크에서 발생하던 보안문제를 동시에 다룰 필요가 있다. 이러한 문제점 및 필요성을 기반으로 oneM2M에서는 사물지능통신에서의 보안 기법 및 전반적인 사물지능통신 기술 플랫폼을 제안하고 있다. 본 논문에서는 oneM2M에서 제안한 사물지능통신 표준 중 보안요구사항 및 대책에 대하여 분석하고, 정리하여 향후 연구에 도움이 되고자 한다. 또한 oneM2M에서 제안한 보안 방안에서 다루지 않는 하드웨어적으로 간과하기 쉬운 요소에 대해서도 추가적으로 고찰해보고 향후 개발할 IoT 보안 플랫폼에 기반지식을 다지고자 한다.

1. 서 론

사물인터넷(IoT)은 정보통신기술(ICT)의 “Any Time”, “Any Place”에 “Any Thing”의 개념이 추가된 것이다.

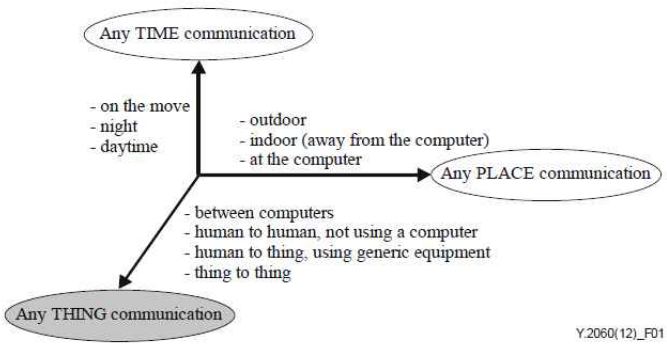

그림 1 IoT 개념도[1]

정보통신기술과 임베디드 시스템의 발달로 기존에 통신 기능이 없던 장치들이 소규모 네트워크를 구성하고 네트워크들을 연결하는 초연결 사회가 도래하였으며, 이로 인해 언제나 어디서나 어떤 것이나 정보를 얻을 수 있게 되었다. 또한, 사물들의 연결은 단순한 정보전달을 넘어서서 빅데이터 분석, 클라우드 컴퓨팅 등 여러 데이터 분석 기법에 의해 가치 있는 정보가 되며 새로운 산업을 탄생시키고 있다.

모든 사물이 통신기능을 통해 서로 연결되고 많은 정보들이 교차됨에따라 사물지능통신(Machine to Machine)의 개념이 등장하였고, 이를 운용함에 있어 정보 전달의 신속성, 신뢰성 등의 다양한 요구사항이 발생하고 있다. 특히, 사물지능통신에서 발생하는 방대한 정보들은 사용자의 지리적 정보나 생활패턴 등의 정보들을 바탕으로 악의적인 정보 가공 및 공급으로 인한 보안문제의 해결이 중요한 문제로 떠오르고 있다. 또한 수많은 장비들이 서로 연결되면서 기존 네트워크에서 발생했던 보안 문제뿐만 아니라, 사물지능통신 네트워크를 구성할 때 사용하는 통신 규격이 상이하여 문제가 발생 할 수 있으므로 IoT에서의 보안 문제는 더욱 신중히 다루어져야 한다.

이러한 문제들을 해결하기 위하여 oneM2M에서는 사물지능통신의 표준규격을 배포하고 기술을 정의 하였다. 표준 규격에는 IoT에 필요한 보안 기술의 요구사항과 그에 따른 보안기법 및 사물지능통신 기술 플랫폼을 제안하고 있다. 본 논문에서는 표준규격 중 보안요구사항에 관한 문서를 분석하고, 나아가 간과하기 쉬운 요소들에 대해 고찰한다.

본 논문은 다음과 같이 구성되어 있다. 2장에서는 oneM2M을 소개하고 보안 요구사항을 분석 및 요약한다. 3장에서는 사물지능통신 보안요구사항 중 하드웨어 보안에 관한 내용을 고찰 하고, 향후 개발할 보안 플랫폼에 대하여 간단히 설명한다. 4장에서 본 논문의 결론과 향후 계획에 대하여 기술한다.

2. IoT 보안 요구사항

2.1 OneM2M

oneM2M은 사물지능통신의 국제 표준화 협력체로 2012년 7월 한국 정보통신기술협회(TTA), 유럽통신표준화기구(ETSI), 국통신정보표준협회(ATIS), 중국통신

Reference	Version	Title
TS 0001	1.6.1	Functional Architecture
TS 0002	1.0.1	Requirements
TS 0003	1.0.1	Security Solutions
TS 0004	1.0.1	Service Layer Core Protocol Specification
TS 0005	1.0.1	Management Enablement (OMA)
TS 0006	1.0.1	Management Enablement (BBF)
TS 0008	1.0.1	CoAP Protocol Binding
TS 0009	1.0.1	HTTP Protocol Binding
TS 0010	1.0.1	MQTT Protocol Binding
TS 0011	1.0.1	Common Terminology

표 1 oneM2M Release 1 specifications[2]

표준협회(CCSA), 일본전파산업협회(ARIB) 등이 참여한 표준 기술을 개발하는 것을 목적으로 한 파트너십 프로젝트이다. 현재는 202개의 파트너와 맴버들이 함께하고 있으며, 2014년 8월 oneM2M Release 1 specifications[2]을 발표하였다.

2.2 Security Requirement

oneM2M Release 1 specifications 중 TS 0002[3]에선 사물지능통신 플랫폼에 대한 전반적인 요구사항을 정의하고 있다. 본 절에서는 TS 0002문서 6.4절의 Security Requirement를 분석 하고자 하며, 그 내용은 다음과 같다.

- 데이터의 기밀성, 무결성, 가용성의 보장.
- USIM(Universal SIM) / UICC(Universal IC Card)이 적용되는 경우 기존의 USIM 및 UICC의 네트워크 계층의 보안 기능을 활용 가능해야함.
- WAN등의 외부연결이나, 일부 기능에 제한을 받는 상황 하에서 M2M간의 연결 중에서 또한 기밀성과 무결성의 보장.
- 자격증명, 상호인증, 권한 관련 부분의 보장.
- 하드웨어 보안 모듈(HSM)을 적용 가능해야함.
- M2M 장비의 하드웨어와 펌웨어의 무결성 보장.
- 인가되지 않은 접근에 대한 방어 대책 지원.
- 보안 자격 증명에 대한 오용, 복제, 대체 또는 도난에 대해 보호할 수 있는 메커니즘의 지원.
- 리플레이 공격이나 신원을 가장하는 공격에 대한 대책의 지원.
- 부인봉쇄 수단의 제공.
- 서비스 제공자와 가입자 간에 보안 보장.
- 표준문서 TR-0008-Security “Analysis of Security Solutions for the oneM2M System”[3] 에서 제시하는 보안위협을 완화해야함.
- 지리적 위치정보에 대한 보안의 보장.

분석 결과를 검토해 보면, 기존의 네트워크 보안 문제에 대한 요구사항을 포함하고 있으며, 이에 더불어 사물지능통신의 지원을 위한 추가부분이 존재함을 알 수 있다. 특히, TR-0008-Security에서는 보안 취약점과 위협에 대한 내용으로 21가지 항목을 명시하고 있으며, 그에 대한 상세 내용은 아래와 같다.

- M2M 장치나 게이트웨이에 저장된, 장기 서비스 키 노출
- M2M 장치나 게이트웨이에 저장된 장기 서비스 키 삭제
- 저장된 장기 서비스 키의 교체
- M2M 기반구조에 저장된 장기 서비스 키 노출
- M2M 기반 구조의 장비에 저장된 장기 서비스 키의 삭제
- M2M 장치나 M2M 게이트웨이에 저장된 민감한 데이터의 노출
- 개체간 M2M 서비스 계층 메시지의 도청
- 개체간 M2M 서비스 계층 메시지의 교체
- 개체간 M2M 서비스 계층 메시지의 리플레이
- M2M 장치 / 게이트웨이에 설치된, 인가받지 않거나 손상된 응용이나 소프트웨어
- M2M 시스템의 상호 의존성에 대한 위협과 그에 따른 영향
- M2M 보안 상황인지
- 도청, 중간자 공격
- 독립적인 보안 요소를 통한 키 이전
- 버퍼오버플로우
- 삽입공격
- 세션 관리와 고장난 인증
- 보안 설정 오류
- 안전하지 않은 암호화 저장
- 유효하지 않은 입력 데이터
- 크로스 스크립팅

TR-0008-Security에서는 이러한 보안 취약점에 대한 해결책 또한 26가지가 명시되어 있으며, 내용은 다음과 같다.

- M2M 기반구조 장비의 장기 서비스키 저장 용도의 시큐어 스토리지
- HSM/서버 HSM에 저장된 접근 불가 속성의 서비스 키
- M2M 장치/게이트웨이의 민감한 기능에 대한 안전한 실행
- HSM과 M2M 장치/게이트웨이 간의 물리적/논리적 연동
- 장기 서비스 키를 접근하는 과정에서의 강력한 인증
- 보안 연계, 상호 인증, 기밀성의 사용
- 중간자 공격에 대한 검증된 방어
- 서비스 계층에 사용하는 세션키의 제한된 수명
- 리플레이 방지
- M2M 서비스 키로부터 유도되는 키
- 일관성 검증
- 정책 기반의 행동
- 공유 자산 인벤토리
- 민감도 평가
- (M2M 시스템에 대한) 위험 평가
- 컨텍스트 인벤토리와 민감도에 대한 평가
- (컨텍스트에 대한) 위험 평가
- 안전한 통신 채널

- 시큐어코딩
- 신뢰할 수 없는 데이터 삽입 방지
- 보안 제어
- 응용프로그램의 깔끔한 구조
- 스탠다드 알고리즘 사용
- 한을 사용하여 저장소 보호
- 화이트리스트

3. 고찰

앞서 살펴본 것과 같이 IoT의 핵심 기술인 사물지능통신 관련 표준인 oneM2M은 사물지능통신에서 필요한 보안 요구사항과 보안 위협 및 대책에 대해 정의하고 있으며, 이는 기존의 네트워크 보안과 유사한 것을 알 수 있었다. 이를 기반으로 본 논문에서는 oneM2M에서 정의하는 표준안의 문제점을 분석하여 추후 IoT 보안 솔루션 및 암호화 모듈 설계에 있어 기반 지식을 마련하고자 한다. oneM2M 표준의 문제점에 대한 분석 결과는 아래와 같다.

3.1 사물별 최적화

oneM2M 표준에서는 전반적인 보안 요구사항 및 해결방안을 제시하고 있으며, 이는 모든 IoT 장치들에게 적용되어야 함을 정의하고 있다. 하지만 IoT는 동기종간의 소규모 네트워크를 구축하여 운용되던 기존 네트워크와는 달리 이기종 장비들이 Mesh 형태로 연결되어 네트워크를 구성되며, 이러한 이기종 장비들은 대부분 특정 목적을 위해 설계된 임베디드 시스템을 기반으로 하고 있다. 이러한 임베디드 시스템 기반의 장치들은 각 목적에 맞는 최적화된 하드웨어 성능을 가지는 특징을 지니고 있으며, oneM2M에서 제시하는 보안 해결방안을 모두 충족시킬 만큼의 자원을 가지고 있지 않은 경우가 대부분이다. 또한, 이러한 oneM2M에서 제시하는 보안 요구사항 및 해결방안을 모두 만족시키는 장치를 개발하기 위해서는 많은 양의 하드웨어 자원이 필요하게 되고, 장치가 수행해야 할 본 목적보다 보안을 위해 할당해야하는 자원의 양이 더 커지게 되는 문제가 발생하게 된다. 따라서, 각 기기들의 목적 및 리소스를 고려하여 표준에서 제시하는 요구사항 중 각 기기들에 필요한 요구사항에 대한 해결책을 선택하여 구현해야 한다.

3.2 하드웨어적 공격

IoT를 구성하는 기기들의 프로토타입 및 시제품 개발을 위해 오픈소스 하드웨가 많이 사용 되고 있다. 오픈소스 하드웨어는 회로 설계 및 성능에 대한 구성을 파악하기 쉽기 때문에 개발에 용이하다. 반면 하드웨어의 구성을 쉽게 파악할 수 있기 때문에 하드웨어 공격에 대해서도 취약할 수 있다. 예를 들어 장치를 파손하지 않고, 소모하는 전력이나 발생하는 전자기파를 분석하여 정보를 추출하는 부채널 공격에 취약할 수 있다. 한편 oneM2M에서 정의하는 표준문서에서는 네트워크 보안에 치중되어 있고 하드웨어 보안에 관한 내용이 미비한 실정이다. 따라서 하드웨어적 공격에 대비한 보안요구사항의 추가가 필요하다.

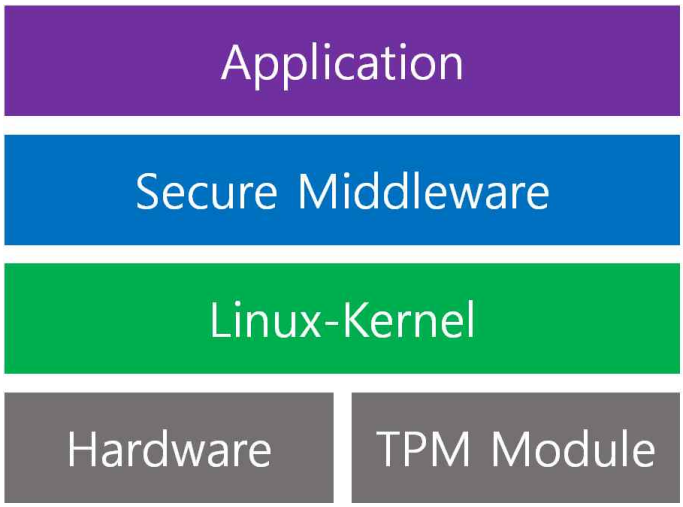

그림 2 Secure IoT Platform Architecture

3.3 Secure IoT Platform

앞 절에서 oneM2M의 표준 보안요구사항을 살펴본 결과 최적화 및 하드웨어적 공격에 대한 방어를 등이 필요한 실정이다. 이점을 인지하고 IoT보안을 실현하기 위해 oneM2M에서 정의하는 표준 보안요구사항 뿐만 아니라, 추가적으로 언급했던 문제들을 해결할 수 있는 Secure IoT Platform을 개발하고자 한다. 새로 개발할 플랫폼은 TPM(Trusted Platform Module)을 활용할 계획이다. TPM은 암호화 키를 저장할 수 있는 일종에 HSM이고, 이를 이용해 본 논문에서 고찰한 IoT 보안을 위한 요구사항을 충족한 플랫폼을 개발하고자 한다.

4. 결론

IoT에 대한 관심이 증가함에 따라 관련 연구나 산업들이 주목받으면서 다양한 요구사항들이 발생하고 있으며, 특히 보안에 관한 문제가 중요하게 대두되고 있다. 이러한 IoT에서의 보안문제를 해결하기 위해 oneM2M에서는 IoT에서 발생하는 보안 요구사항 및 해결방안을 제시하고 있다. 본 논문에서는 oneM2M 표준문서를 분석하였으며, 그 결과 임베디드 시스템 기반의 이기종 기기들의 연결로 구성되는 IoT 환경에서의 서로 다른 목적과 하드웨어 자원을 가지는 기기들에 대한 고려가 이루어지지 않아 보안 최적화 및 하드웨어적 공격과 같은 이슈가 발생할 수 있음을 인지할 수 있었다. 이를 기반으로 향후 진행될 사물지능통신 보안요구사항을 만족하고 최적화된 암호화 모듈의 설계에 있어 기반지식을 마련할 수 있었다.

참고 문헌(References)

[1] ITU-T Y.2060, Overview of the Internet of Things, 2012.6.
[2] http://onem2m.org/technical/published-documents
[3] TS-0002-Requirements
[4] TR-0008-Security