정 보 보 호 학 회 지
제28권 제5호, 2018. 10

안전한 IoT 서비스를 위한 디바이스 보안과 플랫폼 보안 연동

김 해 용*, 지 장 현*, Asep*, 김 호 원**

요 약

사물인터넷 서비스는 다양한 기능과 성능을 갖는 디바이스와 게이트웨이, 플랫폼, 서비스가 서로 상호 연동/통신함으로써 실현된다. 해당 서비스의 안전성 및 신뢰성을 보장하기 위해선 서비스 각 구성 요소에 적절한 보안 기술이 필요하다. 서비스 및 API 수준에서는 OpenID-connect, OAuth2, SAML, XACML과 같은 인증/인가, 접근 제어 기법이 필요하며, 플랫폼 및 프로토콜 수준에서는 MQTT, CoAP, HTTPS, RSPF 프로토콜 및 보안 절차가 필요하다. 한편, 이들 보안 기술은 공통적으로 TLS/DTLS 보안 프로토콜을 사용한다는 특성을 가진다. 이에, 본 논문에서는 사물인터넷의 디바이스, 게이트웨이, 플랫폼에서 손쉽게 사용될 수 있도록 TLS/DTLS 보안 칩 개발 사례를 소개하고 이를 TLS 오픈 소프트웨어 스택인 mbedTLS와의 연동 사례를 소개함으로써 사물인터넷 구성 요소에 공통적으로 활용 가능한 보안 기술 구현 사례를 살펴본다.

Ⅰ. 서 론

현재 사물인터넷은 거의 모든 산업 현장에 활용되고 있다. 최근에는 지능형 사물인터넷으로 진화하여, 데이터 중심의 서비스 지향적으로 발전하고 있다. 사물인터넷이 서비스에서 필요로 하는 데이터/정보를 원활하게 수집/가공/분석/활용/공유하기 위해선 연결성(connectivity)가 가장 중요한 요소이며, 이러한 연결성 적용 대상은 디바이스에서 게이트웨이, 플랫폼, 서비스까지 확대된다. 통신 수준과 데이터 수준에서의 연결성 제공 뿐만 아니라, 보안 관점에서도 end-to-end 보안성을 제공하거나 이에 준하는 형태로 보안성을 제공해야 한다. 이에, 사물인터넷 각 구성요소에 적합한 보안 기술이 표준화되거나 기존 보안 기술을 활용한다.

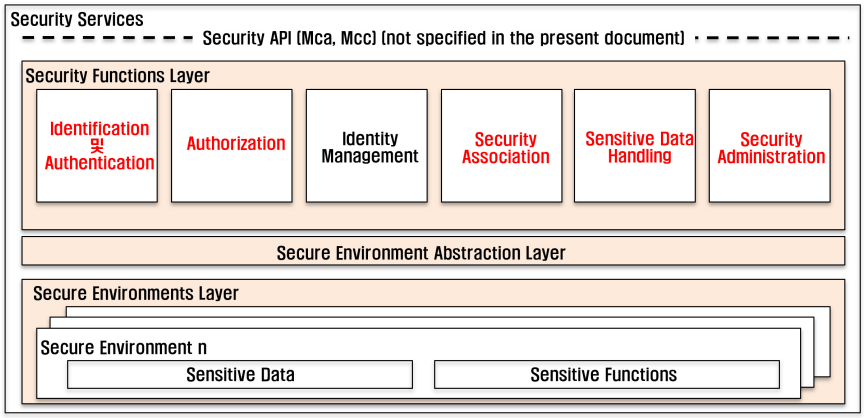
본 논문에서는 기존 사물인터넷 플랫폼에서 제시하고 있는 보안 기술의 특성과 응용 프로토콜/전송 계층 프로토콜에서 사용하는 보안 기술의 특성을 분석하여 이를 효율적으로 실현한 사례를 보여준다. 즉, TLS 전용 보안 칩 개발 사례를 소개하고 이를 TLS 소프트웨어 스택과 연동한 결과를 제시하며, 또한, MQTT, CoAP 응용 프로토콜, oneM2M 플랫폼 보안과의 연동 가능성을 보인다.

본 논문은 다음과 같이 구성된다. 2절에서는 oneM2M 플랫폼에서의 보안 프레임워크와 프로토콜은 TLS 프로토콜을 사용하는 경우가 많으므로 TLS 프로토콜을 효과적으로 사물인터넷 디바이스와 게이트웨이, 플랫폼에 구현하는 것이 필요하다. 3절에서는 TLS 전용 보안 칩 구조를 제시하고 mbedTLS 프로토콜 스택(mbedTLS[2])에 보안 칩을 연동 구현한 사례를 기술한다.

Ⅱ. 사물인터넷 플랫폼 보안 기술

사물인터넷 디바이스와 서비스 등을 연결하는 플랫폼으로는 oneM2M과 같은 국제 표준 플랫폼[1] 혹은 AWS IoT나 마이크로소프트 Azure IoT, IBM Watson IoT, Cisco IoT Cloud Connect, Bosch IoT Suite, Kaa IoT, ThingSpeak 등 다양한 비표준 상용/프리웨어 플랫폼이 존재한다. 이 플랫폼 중에서 oneM2M 플랫폼을 제외한 나머지 플랫폼에서는 보안을 위해 MQTT와 CoAP 보안, TLS, DTLS 보안 기술을 사용한다.

이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구)
* 부산대학교 전기전자컴퓨터공학과 ({ryoung0327, jjh0819, asep.muhamad11}@pusan.ac.kr)
** (교신 저자) 부산대학교 전기전자컴퓨터공학과 (howonkim@pusan.ac.kr)



〔그림 1〕 사물인터넷 플랫폼(oneM2M)에서 제공하는 주요 보안 기술

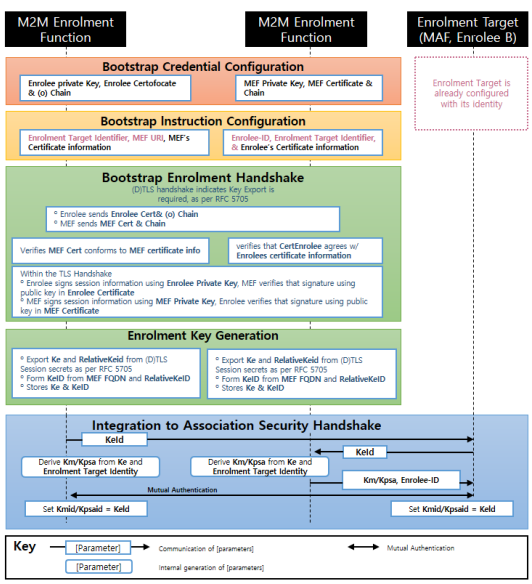
oneM2M 표준에서는 그림 1에서 보는 바와 같이 구성하는 디바이스와 서비스에 대한 식별(identification)과 인증(authentication), 보안 연관(security association), 민감 데이터 처리(sensitive data handling), 보안 관리(security administration) 등 다양한 보안 기술이 표준에서 정의되어 있다.

이는 oneM2M 표준을 주도한 기관이 각국의 통신 관계자 및 표준 기관(ETSI, TTA, ARIB, CCSA, TIA 등)이기 때문에 oneM2M 표준에서는 원격 인증 및 보안 연관 등 다양한 보안 표준을 정의하고 있다.

oneM2M 플랫폼 보안 표준에서는 원격 보안 설정 프레임워크(RSPF[1])(그림 2)와 보안 연관 설정 프레임워크(SAEF[2]) 등, oneM2M 네트워크에 특화된 보안 설정 및 상호 인증 기법을 제시하고 있다. 이 보안 프레임워크에서는 사전 공유한 비밀키 기반 혹은 인증서 기반, MAF(M2M Authentication Function) 기반으로 보안 설정 및 상호 인증을 제공한다.

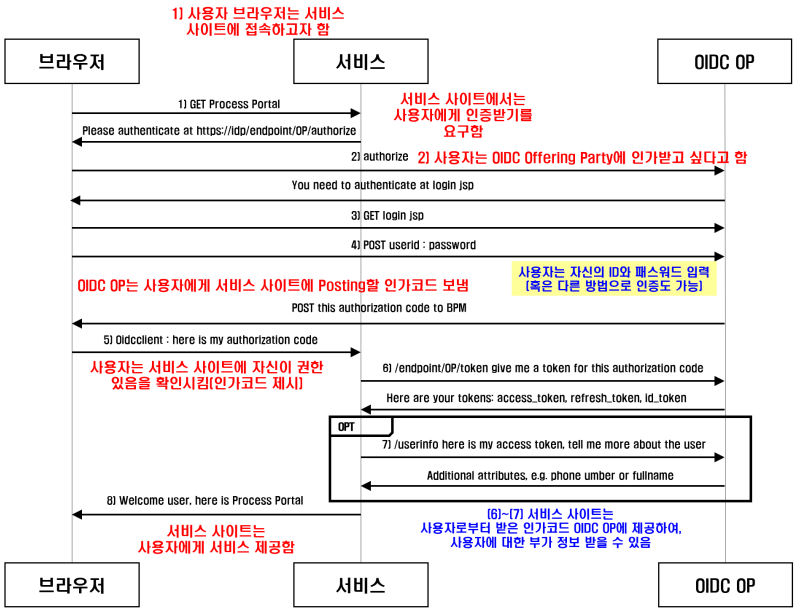
그림 2에 제시된 RSPF 프레임워크는 인증서를 기반으로 RSPF를 수행하는 절차를 보여주고 있다. Enrolee는 Enrolment Target(예: 게이트웨이)와 통신을 원하는 디바이스로 볼 수 있다(디바이스 A로 가정함). M2M Enrolment Function은 oneM2M 상에서 디바이스의 등록 및 인증을 수행해주는 서비스로서 서버에 있다고 가정한다. 각 단계는 다음과 같이 동작한다.

- Enrolee(등록대상 디바이스)는 MEF를 통하여 Enrolment Target(게이트웨이)와 상호 인증을 통해 통신을 하고 싶어함
- 먼저, Enrolment Target(게이트웨이)은 디바이스 A가 연결될 Gateway이며, MEF는 Enrolment Target을 이미 인증했다고 가정함. 또한 각 엔터티는 공개키 암호 시스템(private key, 인증서, 인증 체인 정보 등)으로 설정되어 있음
- 디바이스 A는 대상인 게이트웨이 ID(Enrollment Target ID) 정보와 자신을 등록/인증해 줄 MEF에



〔그림 2〕 oneM2M 플랫폼에서 정의된 원격 보안 설정 프레임워크

1) RSPF: Remote Security Provisioning Framework
2) SAEF: Security Association Establishment Framework



〔그림 3〕 사물인터넷 플랫폼에서 사용가능한 OpenID-Connect 프로토콜

대한 정보(MEF URI)를 알고 있음

- 인증서 기반 상호 인증을 수행함. TLS 상호 인증 기법과 동일함(이때 디바이스와 MEF는 서로 다른 CA로부터 인증서 서명될 수 있으며, 이 경우, 인증 체인을 통해 검증 될 수 있음)
- 등록키 생성단계에서는 디바이스와 MEF가 공유 비밀키 Ke와 해당 ID인 KeID를 갖게 됨. 이때, 게이트웨이는 이미 MEF에 등록되어 있고 인증되어 있음
- 디바이스가 게이트웨이에 연결하고 싶다고 하면서 KeID 정보를 줌. 게이트웨이는 자신을 믿는 MEF 서버에 KeID에 해당하는 키(Ke)를 달라고 함
- MEF 서버는 디바이스 A에 Ke에서 세션키를 발생시키라고 하며, 자신도 동일하게 Kpsa를 생성함. 이때, Kpsa는 게이트웨이와 디바이스 A간의 상호 공유키가 됨
- 이 공유키를 기반으로 디바이스 A와 게이트웨이는 상호 인증을 수행함

위에서 제시된 RSPF 프레임워크는 oneM2M에서 정의된 보안 기술 중에서 가장 복잡한 기술에 속한다. 그런데 해당 기술을 보면 결국 공개키 인증서 기술과 TLS 기반의 상호 인증 기법을 사용함을 볼 수 있다.

oneM2M에서 정의된 보안 기술을 사용하지 않고, 기타 플랫폼에서 사물인터넷 디바이스 혹은 서비스가 다른 사물인터넷 자원에 대한 접근 권한을 얻거나 SSO(Single Sign On) 서비스를 얻기 위해서는 OpenID-Connect([3])와 OAuth2를 함께 사용하여 인증/인가 기법을 통합/연동할 수 있다. 그림 3에서 인증 절차를 수행하는 openID-Connect의 동작 절차를 보면 다음과 같다.

- OpenID-Connect 프로토콜은 디바이스나 사용자, 브라우저, 클라이언트 소프트웨어 등이 자신을 인증하는데 사용될 수 있음
- 우선 사용자(브라우저)는 특정 서비스에 접속하고자 함. 즉, 서비스 사이트에서는 사용자에게 인증이 필요함을 요구함
- 이에, 사용자는 OIDC OP(Offering Party)에 권한을 받고 싶다고 하면, OIDC OP는 사용자에게 자신을 인증하라고 함
- 사용자는 자신의 ID와 패스워드 입력(혹은 그 외, 다양한 인증 기법 사용)하여, 자신을 인증함
- OIDC OP는 인증된 사용자에게 서비스를 접근할 수 있는 인가 코드를 보냄
- 사용자는 이 인가 코드를 사용하여 서비스 접근 권한이 있음을 확인시킴

- 서비스 사이트는 사용자로부터 받은 인가코드를 OIDC OP에 제공하여 사용자에 대한 부가 정보를 받을 수 있음
- 서비스 사이트는 사용자에게 서비스를 제공함

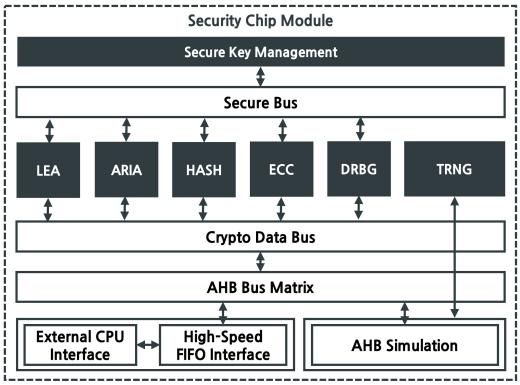
OpenID-Connect 프로토콜은 예시로 제시된 사용자 패스워드 기반의 인증뿐만 아니라, 다른 인증 기법을 프로토콜 내에서 사용할 수 있다. 또한, OAuth2 프로토콜과 함께 사용하면 인증/인가 기능을 제공하게 된다. 여기서 OpenID-Connect에서는 TLS를 사용하지 않지만 OAuth2에서는 TLS를 사용하므로 일반적인 사물인터넷 플랫폼의 인증/인가 기능을 위해선 결국 TLS 프로토콜을 사용함으로 알 수 있다. 다음절에서는 TLS 프로토콜 전용 보안 칩을 설계하고 이를 TLS 소프트웨어 스택과 연동하는 기술을 소개한다.

Ⅲ. TLS 전용 보안 칩과 TLS 프로토콜 연동

사물인터넷 디바이스와 게이트웨이, 플랫폼간 통신 프로토콜인 MQTT, CoAP, HTTPS는 대부분 TCP 혹은 UDP에 기반을 두고 있으며, 이 때문에 보안도 TLS/DTLS을 사용한다. 또한, 본 논문의 2장에서 제시된 것처럼 사물인터넷 플랫폼에서도 상호 인증 및 보안 통신을 위해 TLS/DTLS 프로토콜을 사용하고 있음을 확인했다. 이에, 만약 TLS 전용 보안 칩이 있다면, 경량 사물인터넷 디바이스에서 디바이스 성능에 영향을 받지 않으면서 상호 인증 및 보안 통신을 제공할 수 있을 것이다. 특히, 사물인터넷 응용 현장에서는 하드웨어 모듈만으로도 TLS/DTLS를 지원하게 된다면 높은 편의성을 가지기 때문에 많은 사물인터넷 응용 현장에서 활용될 것이다.

다음 그림 4는 TLS 소프트웨어 스택과 연동되는 저자들이 자체 개발한 보안 칩 블록도를 보여주고 있다. 개발된 보안 칩은 TLS 표준 보안 Cipher Suit (ECDHE-ECDSA-ARIA128-GCM-SHA256)들을 지원할 수 있도록 다양한 대칭키 암호, 타원곡선 암호, 대칭키 암호 동작 모드, 난수 생성기 등을 제공한다. 특히 국내 표준 암호인 블록 암호 2종(LEA, ARIA)을 제공한다.

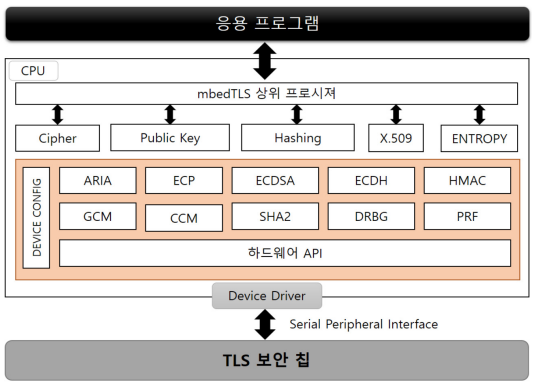
보안 칩은 내부의 비밀키와 외부와 공유되는 키의 데이터패스를 분리(Data Bus 와 Secure Bus로 분리됨)함



〔그림 4〕 TLS 전용 보안 칩 블록도

으로써 보안성을 강화 시켰다. 이 칩을 사용하면 다양한 보안 목적(키교환/인증/암호화/키 관리 등)을 실현할 수 있으며, ARM에서 제공한 오픈 소스 TLS 소프트웨어인 mbedTLS와 완벽한 호환성을 제공한다.

TLS 전용 보안 칩을 mbedTLS와 연동하기 위해선 mbedTLS 하위단 소프트웨어에 대한 수정과 칩 특성을 고려한 연동 API 개발이 필요하다. 그림 5는 TLS 전용 칩과 mbedTLS 소프트웨어 스택간의 연동 구조를 보여준다. 그리고 칩과 TLS 소프트웨어 스택간의 통신은 Serial Peripheral Interface(SPI)를 통하여 이뤄진다. 그림 5를 보면 TLS 전용 보안 칩과 기존 mbedTLS 소프트웨어 연동을 위해 디바이스 드라이버 개발과 하드웨어 API 개발, 그리고 mbedTLS 하위 계층 수정 개발이 필요함을 알 수 있다.



〔그림 5〕 mbedTLS와 TLS 보안칩과의 연동 구조

Ⅳ. 결 론

본 논문에서는 국제 표준 사물인터넷 플랫폼인 oneM2M 표준의 주요 보안 기술을 살펴보았다. 또한, 그 외 비표준 상용 사물인터넷 플랫폼인 AWS IoT, Kaa IoT 플랫폼에서 사용하는 보안 기술에 대해서도 살펴봤다. 이들 플랫폼과 MQTT나 CoAP과 같은 사물인터넷 전용 응용 프로토콜에서는 결국 TLS 혹은 DTLS를 상호 인증 혹은 보안 통신 기본 프로토콜로 사용한다. 이에, 본 논문에서는 저자가 개발한 TLS 전용 보안 칩의 구조와 기존 mbedTLS 소프트웨어 스택과의 연동 구조를 제시함으로써, 사물인터넷 디바이스와 게이트웨이, 플랫폼에서 보안 칩 형태의 하드웨어 모듈의 도움을 받아 사물인터넷의 보안성을 높이는 사례를 살펴봤다.

참 고 문 헌

[1] TS-0003 Security Solutions, Relase oneM2M release 3(3.8.0), technical specifications, April, 2018

[2] mbedTLS software stack site, mbed site, https://tls.mbed.org

[3] OpenID-Connect Use Case site, IBM https://www.ibm.com/developerworks/community/blogs

〈저 자 소 개〉

김 해 용 (Haeyong Kim)
학생회원
2015년 8월 : 부산대학교 전자공학과 학사 졸업
2017년 8월 : 부산대학교 전기전자컴퓨터공학 석사 수료
2017년 9월~현재 : 부산대학교 전기전자컴퓨터공학 박사과정
관심분야 : IoT, 하드웨어 보안, 인공지능, ASIC, 플랫폼 보안

지 장 현 (JangHyun Ji)
학생회원
2016년 2월 : 부산대학교 정보컴퓨터공학 학사 졸업
2018년 2월 : 부산대학교 전기전자컴퓨터공학 석사 수료
2017년 9월~현재 : 부산대학교 전기전자컴퓨터공학 박사과정
관심분야 : IoT보안, 하드웨어 보안, 보안 SoC

Asep Muhamad Awaludin
2015년 8월 : University of Indonesia Physics Instrumentation
2017년 9월~현재 : 부산대학교 부산대학교 전기전자컴퓨터공학 석박사 통합과정
관심분야 : 하드웨어 보안, 블록체인, 보안 SoC

김 호 원 (Howon Kim)
종신회원
1993년 2월 : 경북대학교 전자공학과 (공학사)
1995년 2월 : 포항공과대학교 전자전기공학과 (공학석사)
1999년 2월 : 포항공과대학교 전자전기공학과 (공학박사)
2008년~현재 : 부산대학교 정보컴퓨터공학부 교수
2015년~현재 : 부산대학교 정보컴퓨터공학부 교수
관심분야 : IoT, 블록체인, 강화학습, 디지털트윈, 플랫폼 보안, 암호 프로세서 등