IoT 디바이스를 위한 Arm PSA 기반 보안 플랫폼 설계

정준영 ○ 조진성
경희대학교 컴퓨터공학과
jjy920517@khu.ac.kr, chojs@khu.ac.kr

Design of a Secure Platform for IoT Device based on Arm PSA

Junyoung Jung ○ Jinsung Cho
Department of Computer Science and Engineering, KyungHee University

요 약

Arm PSA는 IoT 플랫폼에서 운용되는 리소스에 대해 실행 환경의 격리를 제공함으로써 기밀성과 무결성을 보장할 수 있는 기술이다. 하지만 PSA 기반 IoT 플랫폼의 개발 및 배포를 위해서는 Arm과 협약을 맺어야 하며, 협약을 맺더라도 IoT 서비스 개발자에게 제한된 정보만 제공할 수 밖에 없다는 문제점이 존재한다. 본 논문에서는 PSA 기반 IoT 보안 플랫폼의 설계와 IoT 서비스 개발자들의 개발 편의성을 위한 API를 제안한다. 이를 위해, IoT 플랫폼의 보안 요구사항을 분석하고 PSA 기반 IoT 보안 플랫폼의 기능을 설계한다.

1. 서 론

일반적인 컴퓨터 시스템 및 IoT에서의 보안 강화를 위해 서비스 실행 환경의 격리를 통한 무결성을 제공하는 TEE(Trusted Execution Environment)가 제안됐다[1]. 그 중 Arm의 TrustZone은 Arm 프로세서 기반 상용 TEE로, SoC(System on Chip)의 하드웨어 및 소프트웨어 리소스를 분할하여 두 개의 영역(Secure world, Non-secure world)에서 보존 및 운영할 수 있다[2]. TrustZone은 모바일 및 IoT 디바이스에 적합한 TEE로 설계됐으며, 사용하는 프로세서 아키텍처에 따라 TrustZone-A와 TrustZone-M으로 구분된다. 저사양 마이크로컨트롤러 용으로 개발되던 TrustZone-M은 2017년 10월 PSA(Platform Security Architecture)라는 명칭으로 새롭게 공개됐다[3].

Arm의 파트너 기업은 PSA를 통해 보안이 강화된 새로운 IoT 플랫폼 및 서비스의 개발을 할 수 있으며, 이를 통해 안전한 IoT 생태계를 구축할 수 있다[3]. 그러나 PSA 적용이 가능한 플랫폼을 개발하기 위해 플랫폼 제조사는 Arm과 NDA(Non-Disclosure Agreements)를 맺어야 하며, 서비스 개발자에게 제공하는 정보가 제한될 수 밖에 없다. 따라서 보안 강화에 대한 가능성이 있음에도 불구하고, PSA를 활용한 IoT 서비스의 연구와 개발이 상대적으로 이뤄지지 않고 있다[4].

본 논문에서는 PSA 기반 플랫폼을 제공하는 단체 및 기업의 입장에서 IoT 서비스 개발자에게 제공할 수 있는 신뢰 플랫폼을 제안한다. 또한, 제안하는 플랫폼을 사용하여 안전한 서비스 개발이 가능한 API를 소개한다. 제안하는 신뢰 플랫폼 및 API를 통해 IoT 서비스 개발자는 플랫폼의 하드웨어 특징 및 보안 알고리즘에 대한 이해 없이, 자유롭게 PSA 기능을 사용할 수 있다.

논문의 구성은 다음과 같다. 2절에서는 PSA와 SE(Secure Element)에 대해 조사한다. 조사 한 내용을 바탕으로 3절에서는 PSA 기반 보안 플랫폼을 설계하고, 4절에서는 결론 및 향후 연구 방향을 제시한다.

이 논문은 2017년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구결과임 (NRF-2017R1D1A1B04035914).

2. 관련 연구

본 절에서는 PSA 보안 모델과 하드웨어 특징에 대해 소개하고, 신뢰할 수 있는 하위 시스템으로써 SE(Secure Element)에 대해 알아본다.

2.1 PSA (Platform Security Architecture)

Arm은 IoT 디바이스의 위협 모델과 보안 분석에 대한 사전 조사를 반영하여 PSA 보안 모델을 설계했다[5]. PSA 보안 모델은 실행 환경의 격리를 제공함으로써 상대적으로 신뢰할 수 없는 플랫폼 리소스가 신뢰할 수 있는 플랫폼 리소스를 손상시키지 않도록 보장하는 것을 목표로 한다[6]. 신뢰할 수 있는 플랫폼 리소스를 PSA Root of Trust(RoT)라 하며, PSA RoT를 보장하는 다양한 격리 방법 중, TrustZone 기반 격리가 있다[7]. TrustZone 기반 격리가 가능한 프로세서는 Armv8-M 패밀리의 Cortex-M23, Cortex-M33이 있으며, 이 프로세서들은 Secure state 혹은 Non-secure state로 실행 가능하다. 두 실행 상태의 구분은 메모리 맵을 통해 이뤄지며, 인터럽트와 예외 처리를 통해 자동으로 전환된다. 이를 위해 SG(Secure Gateway), BXNS, BLXNS와 같은 새로운 명령어가 개발되었고, Secure state 메모리 공간을 나누어 NSC(Non-Secure Callable)라는 메모리 공간이 정의됐다. NSC에는 Non-secure state의 소프트웨어가 Secure state의 리소스에

접근하기 위한 분기점(entry point)이 정의되어 있으며, Non-secure state의 소프트웨어가 잘못된 분기점으로 분기하는 것을 방지하기 위한 명령어가 SG이다. BXNS는 Secure state의 소프트웨어가 Non-secure state의 소프트웨어로 분기하거나 복귀하는데 사용되는 명령어이며, Secure state의 소프트웨어가 Non-secure state의 함수를 호출하기 위한 명령어가 BLXNS이다. 이를 통해 Non-secure state의 소프트웨어는 Secure state와 격리되어 직접적인 접근이 불가능하다.

2.2 SE (Secure Element)

국제 표준 기구인 Global Platform은 IoT 디바이스의 보안 강화를 위해 하드웨어 보안 모듈을 제안하며, SE(Secure Element)를 소개했다[8]. SE는 변조 방지 플랫폼으로 하드웨어 암호화 가속기, TRNG(True Random Number Generator), 안전한 데이터 저장소(e.g., OTP)의 역할을 수행할 수 있다. Arm에서는 PSA 기반 프로세서에 안전한 저장소 및 하드웨어 암호화 가속기가 없을 경우, 신뢰할 수 있는 하위 시스템으로 SE를 사용하는 아키텍처를 제안한다[7]. 이 아키텍처는 민감 데이터 암/복호화 및 저장에 SE를 사용하여, 데이터의 기밀성과 무결성을 증명할 수 있다.

3. PSA 기반 보안 플랫폼

본 절에서는 2절에서 조사한 내용을 바탕으로 PSA 기반 보안 플랫폼 설계를 위한 요구사항을 분석하고 보안 플랫폼의 기능 및 API를 정의한다.

3.1 보안 플랫폼 요구사항

본 논문에서 제안하는 보안 플랫폼은 IoT 기술의 요구사항을 정하는 글로벌 표준 단체, oneM2M의 표준을 준수하여 설계한다. oneM2M의 TS-0002-Requirements 표준 문서에 의하면, M2M(Machine To Machine) 디바이스는 다음과 같은 보안 요구사항을 만족해야 한다[9].

• SER-002: oneM2M 시스템은 데이터의 기밀성을 보장할 수 있어야한다.
• SER-003: oneM2M 시스템은 데이터의 무결성을 보장할 수 있어야한다.
• SER-013: oneM2M 시스템은 부팅 및 런타임 시, 무결성 검사를 위한 메커니즘과 소프트웨어/하드웨어/펌웨어의 업그레이드 메커니즘을 제공할 수 있어야한다.
• SER-064: M2M 장치는 승인되지 않은 소프트웨어/미들웨어/펌웨어의 설치나 수정을 방지하는 메커니즘을 제공해야한다.
• SER-065: M2M 장치는 승인되지 않은 소프트웨어/미들웨어/펌웨어의 설치나 수정을 감시하는 메커니즘을 제공해야한다.
• SER-068: oneM2M 시스템은 암호화 기술을 사용하여 데이터의 인증 및 무결성을 보장해야한다.
• SER-069: oneM2M 시스템은 디지털 서명 등의 방법을 사용하여 데이터를 안전하게 전송할 수 있어야 한다.

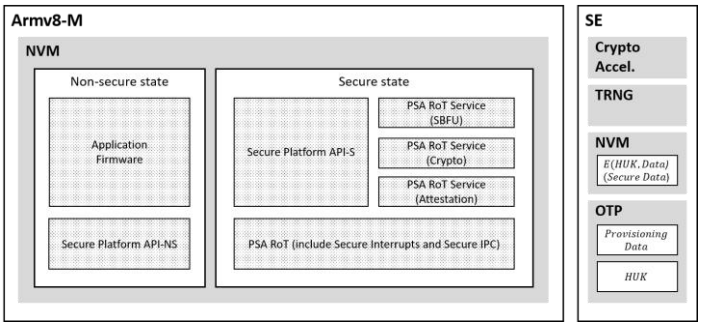

그림 1. PSA 기반 보안 플랫폼

3.2 보안 플랫폼 설계 및 기능

그림 1과 같이 PSA 기반 보안 플랫폼은 Armv8-M 패밀리의 메인 프로세서와 신뢰할 수 있는 하위 시스템인 SE로 구성된다.

메인 프로세서는 NVM(Non Volatile Memory)의 메모리 맵 구성에 의해 Non-secure state와 Secure state로 구분된다. Non-secure state는 IoT 서비스를 위한 어플리케이션 펌웨어(Application Firmware)와 PSA RoT Service의 호출이 가능한 Secure Platform API-NS가 있다. Secure state는 Secure Platform API-NS와 PSA RoT Service의 인터페이스인 Secure Platform API-S, 안전한 인터럽트 및 IPC(Inter-Process Communication)를 제공하는 PSA RoT, 그리고 세 가지의 PSA RoT Service가 있다. PSA RoT Service는 유일하게 SE에 접근할 수 있는 권한을 가지고 있으며, 안전하게 보호되도록 격리된다. PSA RoT Service의 각 기능은 다음과 같다.

• SBFU(Secure Boot & Firmware Update): PSA 기반 플랫폼의 안전한 디바이스 부팅 및 안전한 펌웨어 업데이트 제공 (대응 보안 요구사항: SER-002, SER-003, SER-013, SER-064, SER-068)
• Crypto: PSA 기반 플랫폼의 데이터 암호화 및 복호화 제공 (대응 보안 요구사항: SER-002, SER-003, SER-068, SER-069)
• Attestation: PSA 기반 플랫폼의 신뢰 상태 증명 제공 (대응 보안 요구사항: SER-013, SER-065, SER-069)

SBFU는 보안 플랫폼의 부팅 및 펌웨어 업데이트 시에 동작하는 서비스로, Non-secure state 어플리케이션의 접근이 불가하다. Crypto는 SE를 통해 암호화 키를 관리하는 서비스로, Non-secure state 어플리케이션의 Secure Platform API-NS를 통한 데이터 암/복호화 요청을 수행한다. Attestation은 외부 서버를 통한 보안 플랫폼의 신뢰 상태를 증명하는 서비스로, 서버와 TLS(Transport Layer

표 1. Secure Platform API-NS

Function	Parameter(s)	Description
crypto_hash( )	char* param, int type	데이터 해쉬 요청. • param: Data • type: MD5, SHA1, SHA256, etc
crypto_symmetric( )	char* param, int type, int enc	데이터 암/복호화 요청. (대칭 키) • param: Data • type: AES128, AES256, ARIA, etc • enc: ENCRYPT, DECRYPT
crypto_asymmetric( )	char* param, int type, int enc	데이터 암/복호화 요청. (비대칭 키) • param: Data • type: RSA1024, ECC, ECDSA, etc • enc: ENCRYPT, DECRYPT
attestation_start( )	char* cert	디바이스 검증 요청. • cert: Device certificate

Security)통신을 수행하고 SE에 저장된 인증서를 통해 플랫폼 검증을 수행한다.

SE는 SHA, AES, RSA, ECC 등의 다양한 암호화 알고리즘을 제공하는 하드웨어 암호화 가속기와 난수 생성을 위한 TRNG, 안전한 데이터 저장소인 OTP(One Time Programmable memory) 및 NVM으로 구성된다. OTP에는 플랫폼 제조 과정에서 주입되는 비대칭 암호화 키인 HUK(Hardware Unique Key)와 Provisioning Data(e.g., Device ID, 인증서, 대칭 암호화 키)가 저장된다. NVM에는 메인 프로세서에서 SE에 전달하는 데이터가 Crypto와 HUK를 통해 암호화되어 (Secure Data) 저장된다. (대응 보안 요구사항: SER-002, SER-003)

3.3 Secure Platform API

표 1은 Secure Platform API-NS에 정의된 API 함수 리스트다. Secure Platform API-NS의 함수는 Secure state 및 SE 접근이 불가하여, Secure Platform API-S의 함수를 요청하고 리턴 값을 받아 사용한다. Secure Platform-NS의 함수가 호출되면, Non-secure state에서 Secure-state의 NSC로 분기하고 SG 명령어가 실행되어 올바른 분기점인지 확인한다. 그 후, Secure Platform API-S의 함수로 분기하여 PSA RoT Service를 수행하고, BXLS에 의해 Non-secure state로 복귀한다. 예를 들어, 그림 2는 외부 서버를 통한 디바이스 펌웨어의 무결성 검증 수행 어플리케이션과 해당 어플리케이션에서 사용하는 Secure Platform API에 대한 샘플 코드이다.

4. 결론 및 향후 연구

본 논문에서는 Armv8-M 프로세서와 SE를 사용한 PSA 기반 보안 플랫폼을 설계하고 API를 제안하였다. 이를 통해 IoT 서비스 개발자들은 플랫폼의 특징 및 암호화 기술 연구에 노력을 할 필요없이 쉽게 PSA 서비스를 이용할 수 있다.

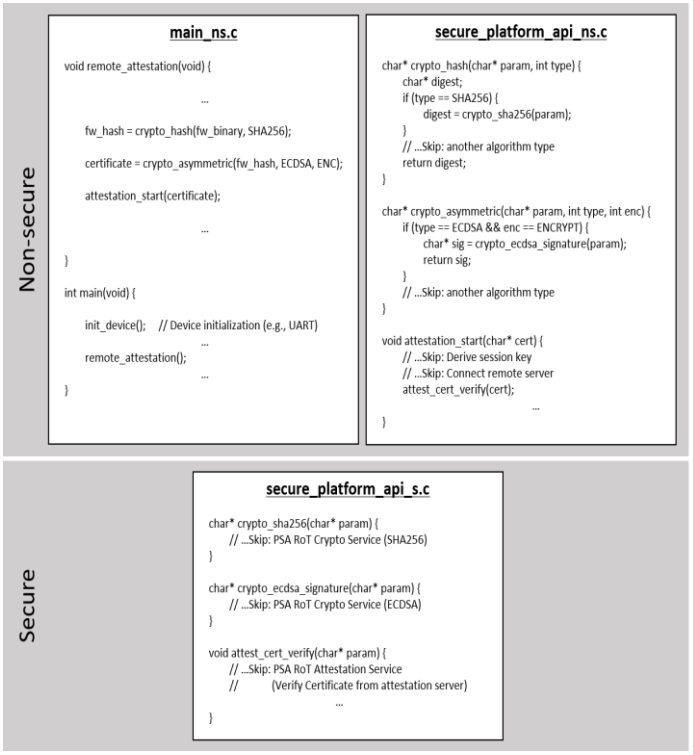

그림 2. Secure Platform API 샘플 코드

향후 연구는 Arm의 FPGA 보드를 사용하여 제안하는 플랫폼과 API를 구현하고, 기존 IoT 플랫폼과 성능 비교 및 분석을 할 계획이다.

참고 문헌

[1] OMTP Limited, “Advanced Trusted Environment: OMTP TR1 V1.1,” 2009.

[2] S. Ray, E. Peeters, M. Tehranipoor and S. Bhunia, “System-on-Chip Platform Security Assurance: Architecture and Validation,” Proc. of the IEEE Vol. 106, No. 1, pp. 21, 2018.

[3] Arm Limited, “Arm Platform Security Architecture Overview Revision1.2,” 2018.

[4] S. Pinto and N. Santos, “Demystifying Arm TrustZone: A Comprehensive Servey,” ACM Computing Surveys, Vol. 51, No. 6, pp. 130, 2019

[5] Arm Limited, “Water Meter Threat Model and Security Analysis (English language Protection Profile) Beta-1,” 2018.

[6] Arm Limited, “Arm Platform Security Architecture Security Model 1.0 Alpha-2,” 2019.

[7] Arm Limited, “Arm Platform Security Architecture Trusted Base System Architecture for Armv6-M, Armv7-M and Armv8-M 1.0 Beta-1,” 2019.

[8] Global Platform Inc, “Secure Elements Configuration V2.0,” 2018.

[9] oneM2M Partners, “TS-0002-Requirements-V4.6.0,” 2019.