ARM TrustZone를 활용한 보안 도어락 시스템*

고병후 ○, 조수연, 조진성(지도교수)
경희대학교 컴퓨터공학과
bhwkd@naver.com, yoy07030@khu.ac.kr

Secure door lock system using ARM TrustZone

Byeonghu Go○, Sueyeon Jo, Prof. Jinsung Cho(Advisor)
Department of Computer Science and Engineering, KyungHee University

요 약

최근 부상중인 IOT 기술 발전의 일환으로 키패드를 누르지 않아도 동작하거나 스마트폰과 연동하여 잠금을 해제하는 등의 기능을 하는 스마트 도어락이 출시되어 많은 곳에서 상용화 되고 있다. 하지만 이러한 스마트 도어락은 민감한 개인정보를 다수 포함하고 해킹의 결과가 치명적인 위험으로 이어질 수 있어 높은 수준의 보안성을 요구한다. 따라서 본 연구는 보안 성능을 높인 스마트 도어락의 구현을 위해 ARM Trustzone의 사용을 제안한다. 또한 하드웨어적 기반이 다른 모바일 기기와 IoT기기 두 단말의 Trustzone간의 보안성을 확보한 통신 방식을 설계한다.

1. 서 론

최근 IOT 기술의 발전의 일환으로 모바일기기를 이용해 자동으로 문을 개폐하는 스마트 도어락의 사용이 증가하는 추세이다. 하지만 이러한 서비스는 해킹공격이 직접적인 신변의 위협으로 이어질 수 있기 때문에 높은 수준의 보안이 요구된다.

본 연구는 특히 hardware적인 보안 위협에 집중한다. 스마트 도어락의 특성상 사용자 인증정보 등 hardware에 저장되어있는 데이터에 대한 보호가 필요하며 암호화 key를 안전하게 저장하는 등 software level의 보안을 더욱 안전하게 지원해 주어야 한다.

따라서 본 연구에서는 모바일 기기를 이용해 문을 개폐하는 스마트 도어락 서비스에 hardware level에서의 보안성을 확보하기 위해 ARM TrustZone의 사용을 제안한다. 스마트 도어락은 두 가지 단말기가 필요하며 각각의 단말은 하드웨어적인 기반이 다르다. 모바일 단은 cortex-A에서의 Trustzone사용을 위해 Android OP-TEE를 사용하며 도어락 단은 cortex-M에서의 사용을 위해 저사양 MCU(microcontroller unit)의 보안플랫폼 PSA를 사용한다. 이를 위해 PSA기반 보안 플랫폼인 KHU-TEE를 사용한다.

2절에서는 본 연구에서 설계한 시스템에 필요한 기술들을 설명하고 3절에서는 서비스를 소개하고 설계한다. 그 후 4절에서 결론 및 향후 개선방안을 제시한다.

2. 관련 연구

2.1 ARM TrustZone

Arm에서 지원하는 보안기술로 하드웨어적으로 일반 실행환경인 REE와 신뢰 실행환경인 TEE로 시스템을 독립시킨다.[1] 보안이 필요한 부분과 그렇지 않은 부분을 독립적으로 구성하여 보안성을 확보한다. 동작 중 normal world에서 secure world로 접근을 요청할 때는 Monitor mode가 사용된다. 본 구성은 GlobalPlatform의 아키텍처를 따른 것이다. TrustZone이 적용된 ARM 사의 프로세서는 크게 ARM Cortex-A 시리즈와 Cortex-M 시리즈로 구분되며 전자는 모바일 환경에 후자는 마이크로컨트롤러가 사용되는 저사양 환경(주로 임베디드)에 사용된다.

2.2 Android OP-TEE

OP-TEE란 주로 모바일을 대상으로 사용되는 ARM의 cortex-A환경의 Linuk kernel에서 Trustzone의 지원을 위해 오픈소스로 제작된 TEE이다. 이 OP-TEE는 GP(GlobalPlatform)을 따른다. Android OP-TEE는 Android os와 호환되도록 이를 적용한 것이다.[2] Android-TEE를 제공하는 Trusty OS를 사용한다. 이를 통해 안드로이드와 동일한 프로세서에서 작동하지만 독립된 하드웨어 환경을 확보할 수 있다.

* "본 연구는 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학 사업의 연구결과로 수행되었음"(2017-0-00093)

2.3 KHU-TEE

PSA기반 보안 플랫폼이다. IoT기기는 저성능의 컴퓨팅환경에서 동작하며 주로 cortex-M을 사용한다. 이러한 환경에서 Trustzone을 지원하기 위해 ARM에서는 저사양 microcontrolier 보안 플랫폼인 PSA를 상용화하였다. 하지만 이를 이용하기 위해서는 ARM사와 NDA를 맺어야하고 개인개발자에게는 사용이 어렵다. 이러한 문제를 해결하고자 개발된 플랫폼이 KHU-TEE다. PSA의 Secure Platform Service를 호출하기 위해 KHU-TEE에서 제공하는 Secure Platform Service API를 이용하여 간단한 개발이 가능하다.[3] 본 연구에서는 기존의 PoC를 위한 환경인 Nuvoton의 NuMaker-PFM-M2351 보드 사용을 가정한다.

2.4 PGP

인증, 기밀성, 무결성의 보장을 위한 일련의 프로세스이다. Hash, 대칭키 암복호화, 비대칭키 암복호화가 사용된다. 두 단말이 비대칭키 쌍인 개인키와 공개키를 각각 공유한다. 이후 대칭키를 사용한 세션키를 공유한다. 송신자가 이후 전송 대상이 되는 데이터를 Hash하고 개인키로 암호화해 전자서명을 만든다. 전자서명과 원본 데이터를 세션키로 암호화하여 전송한다. 수신자는 이를 복호화 하고 전자서명을 복호화하여 인증을 완료한다. 그리고 복호화된 원본 데이터를 Hash하여 전자서명과 비교해 무결성을 검증한다.

3. 시나리오 제안 및 구현

3.1 문제 정의

기존 스마트 도어락을 Trustzone을 이용하여 보안성있게 설계한다. 이를 위해 도어락 단과 모바일 단에서 필요한 application과 data들을 그 보안적 민감성에 따라 구분하여 Secure world와 Non secure world에 위치시킨다. 또한 TEE영역 밖에서 민감한 데이터는 암호화되어 처리될 수 있도록 전체 동작 시나리오를 설계한다.

3.2 시스템 제안

시스템은 크게 도어락 단과 모바일 단으로 나뉘어진다. 도어락 단은 cortex-M 환경을 상정하여 Non secure영역의 FreeRTOS와 Secure영역의 KHU-TEE로 구성된다. 모바일 단은 cortex-A환경에 적용하기 위해 Non secure영역의 Android os와 secure영역의 Android OP-TEE로 구성된다. 각 단말에서 TEE영역은 REE영역에 접근할 수 있고 REE는 정해진 interface를 통해서만 TEE에게 처리를 요청한다. 각 단말의 통신은 오로지 REE영역끼리의 송수신으로 이루어지고 이는 Ad hoc모드의 Wi-Fi통신을 사용한다.
암호키, 사용자 정보는 모두 TEE영역에서 처리된다. REE 및 송수신 채널에서는 암호화된 상태로 처리된다. 암호화 및 인증 프로세스는 PGP를 따르며 RSA, AES, SHA-256을 이용한다. 사용자 PW, 암호키와 같이 민감한 데이터는 모바일 단의 경우 TEE영역의 Flash Memory에 저장된다. 하지만 도어락단은 그 용량의 문제로 REE영역에 파일형태로 암호화하여 저장하고 해당 암호키만 TEE에 저장해 둔다. 이때 암호화에 필요한 기능은 그 안정성의 보장을 위해 openssl을 이용하여 구현한다.

표 1 module structure

		Module	Function
도어락	REE	통신 모듈	모바일단과 데이터 송수신한다.
		도어락 어플리케이션	TEE영역에 데이터 저장, 처리, 반환 요청한다.
	TEE	암호키 관리 모듈	암호키를 관리하고 유효기간이 지나면 이에 대한 처리를 요청한다.
		암복호화 모듈	암호키와 plain text를 받아 암호화하여 반환한다. 혹은 복호화 한다.
		사용자 확인 모듈	도어락 어플리케이션으로부터 사용자 확인이 요청되면 이를 수행하고 결과를 반환한다.
		문 개폐 모듈	문 개폐 명령을 확인하고 올바른 사용자이면 수행한다.
모바일 기기	REE	통신 모듈	도어락 단과 통신을 수행한다.
		사용자 어플리케이션	UI를 제공하고 TEE영역에 데이터 저장, 처리, 반환을 요청한다.
	TEE	암호키 관리 모듈	암호키를 관리하고 유효기간이 지나면 이에 대한 처리를 요청한다.
		암복호화 모듈	암호키와 plain text를 받아 암호화하여 반환한다. 혹은 복호화 한다.
		사용자 인증 모듈	사용자 정보를 저장하여 사용자 어플리케이션으로부터 인증요청이 들어오면 이를 수행하고 결과를 반환한다.
		도어락 등록 모듈	도어락의 고유번호를 관리하고 해당 데이터를 CRUD한다.

3.3 동작 시나리오

3.3.1 모바일단 사용자등록 시나리오

모바일 단에서 사용자 등록을 위해 ID, PW를 입력받는다. 동시에 RSA 기반 비대칭키 쌍이 생성되어 유저정보, 비대칭키가 key, value 쌍으로 TEE에 저장된다. 이후 사용자는 본인 인증을 위해 ID, PW를 입력하여 TEE에서 인증을 완료한 뒤 허가 메세지가 REE로 전달되면 application을 사용한다.

3.3.2 사용자, 도어락 상호 등록 시나리오

도어락단과 모바일단이 상호간에 정보를 등록하고 암호키를 교환한다. 해당 단계는 **그림2**와 같다. 사용자, 도어락 등록 모드가 실행되고 Ad hoc모드로 도어락단과 모바일단이 통신을 준비한다. 이러한 통신을 위한 application은 REE에 위치한다. 이후 두가지 전송, 확인 과정을 거친다.
(1) 공개키를 도어락으로 전송한다.
도어락은 수신 상태 메시지와 도어락의 고유번호를 응답한다.
(2) 사용자 정보 및 대칭키를 전송한다.
모바일 단에서 REE의 사용자 application은 TEE영역에 도어락 등록을 위한 사용자 정보와 대칭키를 요청한다. TEE에서는 AES대칭키를 생성하고 대칭키와 ID를 개인키로 암호화하여 REE로 반환한다. 이후 이 암호문은 도어락 단으로 전송된다. 이후 도어락 단에서는 받은 암호문을 TEE로 넘겨주고 복호화, 인증, 무결성 검사가 끝나면 REE로 완료됨을 반환한다.

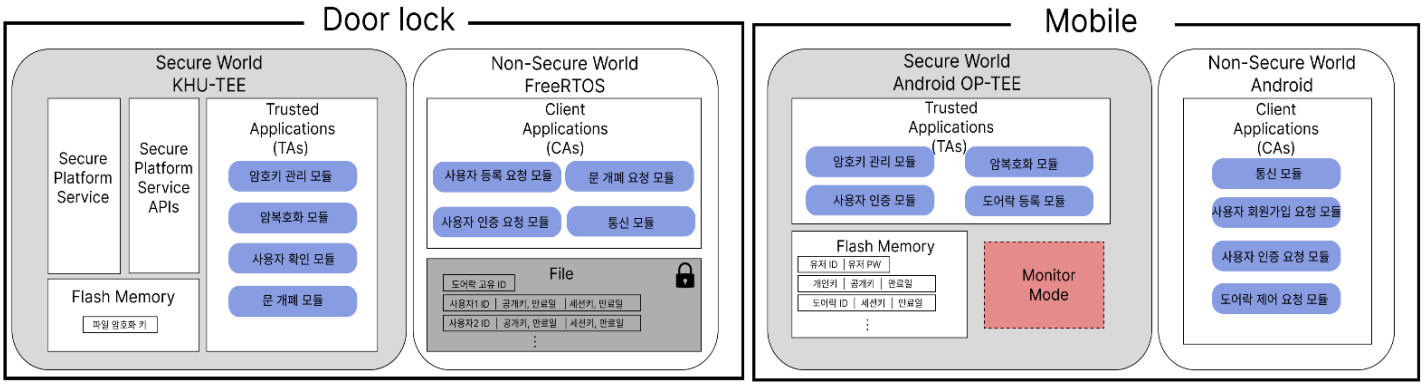

그림 1 system architecture overview

위의 과정이 끝나면 도어락 등록이 완료된다. 성공 메시지가 안드로이드 단으로 도착하여 등록이 완료되면 등록모드는 종료된다. 등록모드 종료 후에 모바일 단에는 도어락 고유번호와 세션키가 매칭되어 저장되고 도어락 단에는 사용자 정보(ID)와 세션키, 공개키가 매칭되어 저장된다.

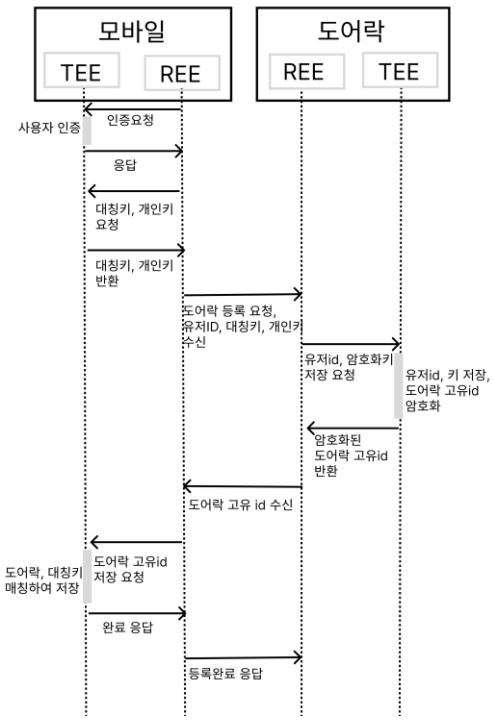

그림2 sequence diagram

3.3.3 도어락 개폐 시나리오

사용자는 OP-TEE 영역에서 ID, PW 기반의 사용자 인증을 진행한 후 도어락 개폐를 시도한다. 그 후 사용자의 키 유효기간을 확인한다. 키가 유효하다면 개폐명령 정보를 SHA-256 해시 알고리즘을 적용한 뒤 개인키로 암호화하여 인증서를 만들고 개폐명령과 인증서를 세션키로 암호화하여 암호문을 REE로 반환하고 REE에서 도어락 단으로 전송한다.

도어락은 암호문을 수신한다. 전달받은 암호문을 KHU-TEE 영역으로 전달해 인증과 무결성 검사를 수행한다. 이후 문 개폐를 수행한다.

4. 결론 및 향후 연구

본 논문에서는 기존 스마트 도어락 시스템에 ARM TrustZone을 적용해 hardware level의 보안성을 높이고 다른 하드웨어 환경의 두 단말의 TEE 영역간 안전한 데이터 통신 프로세스를 제안하였다. 이를 통해 도어락 뿐만 아니라 높은 보안 레벨이 요구되는 잠금 장치로의 적용을 기대할 수 있다.

향후 본 연구는 사용자 인증 방식을 확장하는 방향으로 진행된다. 현재는 모바일단에서 ID, PW를 입력 받는 것에서 그치지만 지문인식, 페이스 아이디를 사용할 수 있고 또한 모바일 단에서 도어락의 출입기록을 확인하고 출입한 사람의 이름을 조회하는 등 여러 유용한 기능으로 확장을 시도한다.

참고 문헌

[1] 손희승, 조진성(2019), 「ARM TrustZone을 이용한 AUTOSAR CSM 설계」
[2] 정준호, 조진성(2020) 「OP-TEE를 통한 안전한 안드로이드 어플리케이션 개발 환경 구축」
[3] 정준영, 조진성(2020) 「KHU-TEE: ARM PSA 기반 IoT 보안 플랫폼」
[4] 서기수(2017), 「ARM TrustZone을 위한 코드 자동 분리 기술」