

IoTivity 프레임워크 기반 안전한 스마트 택배함 시스템 설계 및 구현

강태규[○] 김병선 장준호 조원희 조진성
경희대학교 컴퓨터공학과

bestbefore@naver.com, ykbs0903@khu.ac.kr, jjh920415@naver.com,
candy_cane_@naver.com, chojs@khu.ac.kr

Design and Implementation of IoTivity Framework-based Secure PostBox System

Taekyu Kang[○] Byoungseon Kim Junho Jang Wonhee Cho Jinsung Cho
Dept. of Computer Engineering
Kyung Hee University

요 약

IoT 발달로 각광받고 있는 스마트 택배함 서비스의 안전한 서비스 제공을 위해서는 디바이스 보안 측면을 고려한 스마트 택배함 시스템 설계가 필요하다. 본 논문에서는 IoT 디바이스 보안 플랫폼을 기반으로 스마트 택배함 시스템을 제시한다. 제시한 시스템은 IoTivity 기술을 기반으로 디바이스간 원활한 데이터 통신을 제공하고, 보안 하드웨어 칩을 기반으로 각종 시스템 보안 기능과 함께 서비스 보안 기능을 제공함으로써 높은 보안성을 보장한다.

1. 서 론

최근 IoT 기술의 금융, 헬스케어, 실생활 등 다양한 분야에 접목되고 있다. 그 대표적인 예로, IoT 기술과 택배 서비스가 결합된 스마트 택배함 서비스 분야가 각광받고 있다. 스마트 택배함은 택배 보관함을 집 앞에 설치하고, 외부에 노출된 비밀번호나 마스터키가 아닌 사용자가 어플리케이션을 이용한 원격 개폐로 편리하고 안전하게 택배를 받을 수 있는 서비스이다.

한편 IoT 기술이 확산됨에 따라 디바이스 보안에 대한 우려가 커지고 있다. 만약 디바이스 보안 이슈가 고려되지 않은 IoT 디바이스가 택배함에 탑재될 경우, 펌웨어 불법 교체, 악성코드 삽입 등의 각종 보안 위협에 노출될 것이고, 사용자의 신체적·물질적 피해를 발생시킬 수 있기 때문에 스마트 택배함의 디바이스 보안 이슈는 반드시 해결되어야 할 문제이다. 이러한 문제를 해결하기 위해 본 연구진은 선행 연구로써 리눅스 기반 고성능 IoT 디바이스를 위한 디바이스 보안 플랫폼을 개발하였다.

본 논문에서는 앞서 언급한 IoT 디바이스 보안 플랫폼을 기반으로 스마트 택배함 시스템을 설계 및 구현하였다. 제시하는 시스템은 IoT 디바이스간 상호 운용성 보장을 위한

IoTivity 프레임워크를 활용하여 디바이스간 접속이 용이하고, TPM 을 기반으로 시스템 및 서비스 수준의 높은 보안 기능을 제공한다.

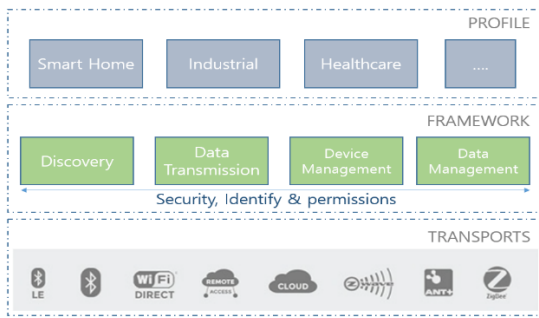
본 논문의 구성은 다음과 같다. 2장에서는 IoT 디바이스 보안 플랫폼 및 IoT 소프트웨어 플랫폼에 대해 살펴본다. 3장에서는 제시하는 시스템에 대해 설명하고, 이에 대한 구현 결과를 4장에서 다룬다. 마지막으로, 5장에서는 향후 연구를 기술하고 결론을 맺는다.

2. 관련 연구

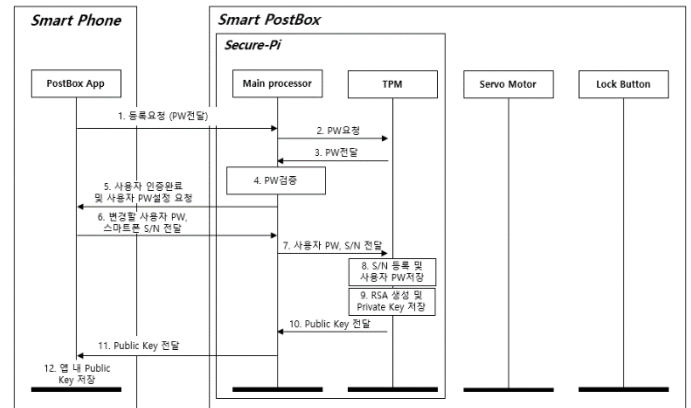
본 장에서는 선행연구로써 개발된 IoT 디바이스 보안 플랫폼의 시스템 보안 기능과 IoTivity 개념 및 아키텍처 대해 살펴보도록 한다.

2.1 IoT 디바이스 보안 플랫폼

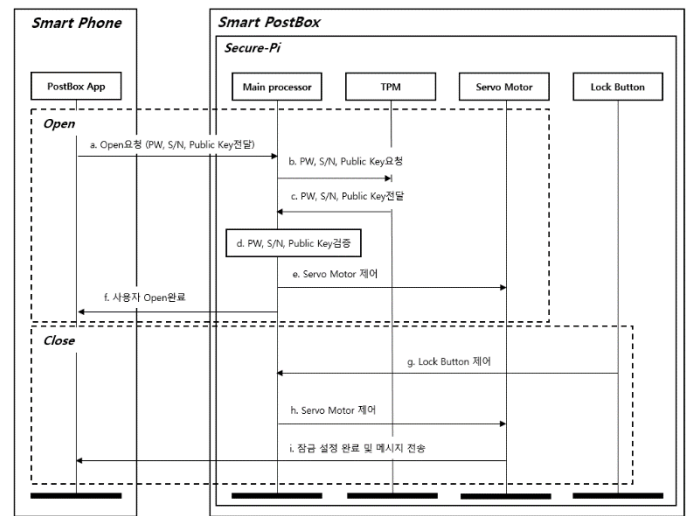
IoT 디바이스 보안 플랫폼(이하 Secure Pi)는 하드웨어 보안 칩인 TPM을 기반으로 아래와 같은 시스템 보안 기술을 제공한다.



[그림 1] IoTivity 아키텍처



[그림 2] 사용자 등록 모드 동작 흐름도



[그림 3] 사용 모드 동작 흐름도

• Secure Key Storage & Management

: 암호화 키를 안전하게 보관 및 관리하기 위한 기술

• Secure Boot: 펌웨어 무결성을 보장하기 위한 기술

• Secure F/W Update: 안전한 펌웨어 업데이트 지원 기술

• Remote Attestation: 디바이스의 신뢰 상태 증명 기술

• Secure Communication: 디바이스 간 안전한 통신

• Mandatory Access Control: 보안 레벨 기반의 접근 제어

• File System Integrity: 파일 시스템 무결성 보장 기술

• File System Encryption: 파일 시스템 기밀성 보장 기술

위 보안 기술을 통해 본 디바이스 플랫폼은 oneM2M 보안 요구사항을 만족함과 동시에 시스템 수준의 높은 보안성을 보장한다.

2.2 IoTivity 오픈소스 프레임워크

IoT 생태계 활성화를 위해서는 IoT 디바이스 간 연결성을 얼마나 쉽게 제공할 수 있는가가 중점이 된다. IoTivity는 이러한 요구사항을 만족시키는 프레임워크로 IoT 디바이스 간 뛰어난 연결성을 보장하는 오픈소스 소프트웨어 기술이다.

IoTivity 프레임워크는 클라이언트, 서버 그리고 모두(클라이언트+서버) 모드로 동작할 수 있다[5]. 일반적으로 사물은 자신의 리소스와 관련된 서비스를 제공하므로 서버 모드로 설정된다. 반면, 디바이스 앱 또는 클라우드 서비스는 사물의 상태를 요청하여 읽어오거나 사물의 설정 변경을 요청하는 형태로 사용되므로 클라이언트 모드로 설정되어 사용된다.

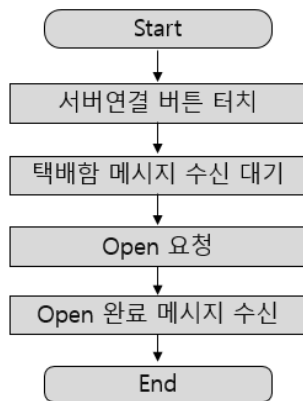
[그림 1]는 Transport, Framework, Profile 계층으로 분류된 IoTivity 아키텍처를 나타낸다. 먼저, Transport 계층에서는 Bluetooth, Wi-Fi, Zigbee 등 다양한 연결 기술을 포함하고 있으며, Framework 계층은 Transport 계층 기술을 기반으로 리소스 발견, 데이터 전송, 디바이스 관리, 데이터 관리 등의 기능을 지원한다. 마지막으로, Profile 계층은 각각의 IoT

분야를 표현한다. Transport 계층과 Profile 계층은 각각 새로운 통신 기술과 새로운 프로파일 적용을 통해 지속적인 확장이 가능하도록 설계되었다.

3. 제안하는 시스템

제안하는 시스템은 크게 스마트폰과 Secure Pi를 탑재한 스마트 택배함으로 구성된다. 본 시스템 동작은 택배함 초기 설정을 위한 <서비스 등록 단계>와 택배함 서비스 제공을 위한 <서비스 사용 단계>로 구분된다.

• **사용자 등록 단계 (그림 2 참고):** 사용자는 스마트폰을 통해 스마트 택배함 리소스를 탐색하고, 사용자 인증을 위한 초기 패스워드(PW)를 입력하여 사용자 등록을 요청한다(1). Secure Pi 내 주 프로세서는 TPM에 저장된 PW를 로드하고(2), PW와 사용자 등록 PW를 비교를 통해 사용자 인증 절차를 수행한다(4). 인증 절차가 완료되었다면, 스마트폰 앱에게 <서비스 사용> 단계에서 사용할 사용자 PW 변경을



[그림 4] 디바이스와 택배함과의 리소스 전송 순서도

요청한다(5). 변경할 PW를 입력하고, 스마트폰 앱은 PW와 스마트폰의 고유 코드를 전달한다(6). 메인 프로세서는 사용자 PW와 고유 코드를 TPM에 전달한다(7). TPM은 전달받은 PW와 고유코드를 NV Storage에 저장한다(8). 시리얼 코드에 대응하는 RSA 키 쌍을 생성하고, Private Key를 저장한다(9). (10), (11)을 통해 Public Key를 스마트폰에 전달하고, PostBox 앱은 Public Key를 저장한다(12).

• 서비스 사용 단계 (그림 3 참고): 사용자 초기 등록 이후, 서비스 사용 단계는 크게 잠금 해제, 잠금 설정의 세부 단계로 구분된다.

사용자는 PostBox 앱을 통해 PW를 입력하여 인증을 요청한다(a). PostBox 앱은 입력된 PW와 스마트폰의 고유코드를 사전에 택배함으로부터 전달받은 Public Key로 암호화하고, 택배함에 전송한다. 메인 프로세서는 TPM의 Private Key를 통해 복호화를 수행하고(b), TPM 내 NV Storage에 보관된 PW, 고유코드로 사용자 인증 과정을 수행한다(c). 인증이 완료되었다면(d) Secure Pi에 연결된 서버 모터를 통해 택배함의 잠금 기능을 해제한다(e). 스마트폰에게 Open 완료 메시지를 전달한다(f).

Lock 버튼을 눌러, 서버 모터를 제어하여 택배함을 닫고, 잠금완료 메시지를 스마트폰에게 전달한다(g~i).

[그림 4]는 사용자가 택배함을 제어하기까지 순서를 설명한다. 기존의 등록된 디바이스일 경우, 사용자 비밀번호와 Public Key를 통하여 인증 절차를 거친 후 인증 완료메시지를 수신받으면, Open 요청을 하여 택배함의 잠금 기능을 해제한다. 택배함으로부터 Open 완료 메시지를 수신한다.

택배함은 TPM을 기반으로 각종 시스템 보안 기능 및 기존 택배 시스템의 인증되지 않은 디바이스가 제 3자에 의해 조작 및 변조하여 택배를 손상 및 도난으로부터 미연에 방지한다.



[그림 5] Secure-Pi와 디바이스간 통신 결과

4. 구현

택배기사가 주인에게 잠금해제를 요청하면, 앱에서 “Open”버튼을 통하여 택배함을 열어주고, “Lock”버튼을 눌러서 배송을 완료한다.

IoTivity Framework의 기본 예제인 simple server와 simple client를 통하여 Secure-Pi와 디바이스간 통신이 이루어졌다.

5. 결론 및 향후 연구

IoTivity 프레임워크를 활용하여 IoT 디바이스간 원활한 데이터 통신을 제공하며, TPM 을 기반으로 각종 시스템 보안 기능과 서비스 보안 기능을 제공함으로써 보안성을 보장한다.

택배함의 서비스 측면에서 발생할 수 있는 보안 문제를 고려하여 더욱 완성도 높은 스마트 택배함을 구현할 계획이다.

* 본 연구는 미래창조과학부 및 정보통신기술진흥센터(IITP)에서 지원하는 서울어코드활성화지원사업(2011-0-00883)과 SW중심대학지원사업(2017-0-00093)의 지원으로 수행되었음.

참 고 문 헌

- [1] CMS WiRE, Top 5 Internet of Things Security Concerns, <http://www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php>
- [2] IoTivity Home, <https://www.iotivity.org/about>
- [3] 박유리 등, “인터넷의 진화와 사회경제적 패러다임 변화연구: 사물인터넷을 중심으로”, KISDI, 기본연구1501(2015.11.)
- [4] 김병선, 조진성, “Secure Pi: COTS IoT 디바이스 보안 플랫폼,” 한국정보과학회 동계학술대회, 2015.12.
- [5] 이원석, 차홍기, 전종홍, 사물인터넷 오픈소스 기술-IoTivity, http://www.kics.or.kr/Home/UserContents/20151215/151215_164143170.pdf