스마트폰을 활용한 IoT 서비스에서의 보안에 관한 연구

김효진
성균관대학교 컴퓨터공학과
e-mail: khdhmshj@skku.ac.kr

A Study on Security of IoT Based on Smartphone

Hyo-Jin Kim
Dept of Computer Engineering, Sungkyunkwan University

요 약

본 논문에서는 IoT 기술 및 스마트폰을 활용한 IoT 서비스에 대한 보안 위협요소를 알아보고 보안 요구사항을 제시한다. 스마트폰을 활용한 IoT 서비스는 스마트폰 자체 내장 센서를 활용한 경우와 외부 센서로부터 정보를 받는 경우가 있다.

1. 서론

IoT(Internet of Things)는 2005년 ITU의 SPU 보고서를 통해 처음 소개된 개념으로 사람과 사물, 사물과 사물 간의 통신을 가능하게 하는 기술이다.[1] 사물에 센서/통신기능이 가능하게 함으로써 사람의 개입 없이 스스로 정보를 수집하고 공유, 처리가 가능한 지능형 글로벌 네트워크 인프라라고 볼 수 있다.

IoT 시장이 빠르게 성장하고 IoE(Internet of Everything)로 가고 있다. 모바일 디바이스와의 연동이 중요시 되고 있고, 그 중에서 사용자의 접근성이 좋은 스마트폰을 활용한 IoT 서비스도 활발히 이루어지고 있다. 하지만 스마트폰의 보안 위협 또한 계속되고 있다. 이러한 보안위협으로 인해 개인정보 유출 뿐 아니라 IoT서비스를 이용함에 따라 정보조작에 따른 부작용을 발생시킬 수 있다. 본 논문에서는 IoT 기술을 소개하고, 스마트폰을 활용한 IoT 서비스에서의 보안 위협과 보안 요구사항에 대해 살펴본다.

2. IoT

IoT는 크게 사람과 사물, 서비스로 이루어진다.
주요 요소 기술로는 센싱 기술, 유무선 통신/네트워킹 기술, 서비스 인터페이스 기술이 있다.[2]

2.1 IoT 요소

2.1.1 사람과 사물

사람은 독립적 주체로서의 의미를 가지고, 사물은 데이터를 추출하고, 추출한 데이터를 전송할 수 있도록 통신이 가능한 것을 말한다. 통신/네트워크 장치를 장착한 사물을 의미한다고 볼 수 있다. 전구, 가습기 등의 유형의 사물과 GPS, 가속도 센서 등을 가진 스마트폰도 사물에 해당된다.

2.1.2 서비스

IoT에서의 서비스란 사물로부터 추출되고 네트워크를 통해 전송된 정보를 분석/처리하여 의미가 있는 정보로 만드는 프로세스와 동작 메커니즘의 집합을 의미한다. 습도계에서 수집된 습도 정보를 이용하여 습도가 낮으면 가습기를 작동시키고, 습도가 적정상태라면 가습기 작동을 중단시키는 동작 등을 서비스의 한 예로 들 수 있다.

2.2 IoT 주요 요소 기술

2.2.1 센싱기술

온습도, 열, 조도, 위치, 모션 센서 등의 물리적 센서와 RFID 등을 이용하여 주변 환경으로부터 정보를 추출하는 기능을 말한다. 또한 물리적으로 존재하지 않고, 스스로 센서 데이터를 발생시키지 않으며, 기존의 다양한 소스와 센싱한 데이터로부터 보다 의미 있는 정보를 추출하는 가상 센싱 기능도 포함된다.

2.2.2 유/무선 네트워킹 기술

IoT의 유•무선 통신 및 네트워크 장치로는 Ethernet, WPAN, Zigbee, Bluetooth, WiFi, 2G/3G/LTE, BcN, PLC 등이 사용된다.

2.2.3 서비스 인터페이스 기술

인간, 사물, 서비스를 응용 서비스와 연동하는 역할을 수행한다. 센서로부터 정보를 얻고, 얻은 정보를 가공/처리하여 원하는 유의미한 정보를 추출하여 IoT 서비스를 제공할 수 있도록 하는 기술이다. Text analytics, Data

fusion, 데이터마이닝 등의 기술을 예로 들 수 있다.

2.3 IoT 관련 동향

<표 1> IoT 관련 동향

미래창조과학부	'사물인터넷 표준화 협의회' 구성 국내 사물인터넷 기술이 세계 표준으로 채택되도록 하기 위함
삼성전자	SAMI(Samsung Architecture for Multimodal Interactions) 프로젝트 진행
SKT	세계적인 반도체 설계 업체 영국 ARM과 손잡고 사물인터넷 플랫폼 공동 연구
SGA	사물인터넷 보안솔루션 개발 중 시큐어 OS 기반 보안솔루션/X86기반의 CPU가 들어있는 임베디드 보안 솔루션

2.4 IoT 서비스 및 응용사례

2.4.1 LG 홈챗(HomeChat) 서비스

2014 CES에서 LG전자가 IoT기술을 구현한 LG 홈챗 서비스 동영상을 공개하였다. LG 홈챗 서비스는 냉장고, 세탁기 등의 가전제품과 스마트폰을 연동하여 제공된다. 스마트폰 메신저를 통해 다른 사람과 채팅하듯 가전제품과 채팅을 하고, 채팅 내용을 기반으로 가전제품이 스스로 작동하게 되는 서비스이다.

그 외에 2014 CES에서 소개된 IoT 제품 및 서비스들은 다음 <표 2>와 같다.

<표 2> 2014 CES에서 소개된 IoT 제품 및 서비스

회사명	제품명	서비스
Belkin	Crock-Pot	Belkin에서 공개한 앱으로 제어 가능한 조리기구
	WeMo	WeMo 앱을 통해 에너지 관리가 가능한 콘센트
Kolibree	Smart toothbrush	자이로미터와 가속계를 이용하여 양치질 효과의 정도를 측정
Withings	Aura	스탠드형 숙면 도움 기기로 온도, 조도 센서 등을 활용하여 침실 환경 조정
Lumo	LumoLift	자세 교정을 위한 센서로 나쁜 자세를 취했거나 한 자세로 너무 오래 있는 경우 진동으로 알림
Sen.se	Sense Mother& Motion Cookies	종합 데이터 수신기 '마더'와 센서 '쿠키' 4개로 구성된 홈네트워크 제품. 소형 센서를 백팩, 알약 등에 고정하여 이동, 사용여부 등의 데이터 수집/통계 및 분석.

3. 스마트폰을 활용한 IoT 서비스에서의 보안위협

3.1 보안 위협

3.1.1 단말

스마트폰은 다른 전자 기기에 비해 도난 및 분실의 위험이 크다. 도난, 분실이 발생한 경우 개인정보 유출의 위험과 비인가 사용자가 IoT 서비스에 접근할 위험성이 있다. 스팸문자, 악성사이트를 통해 유입되는 악성코드의 위험성도 있다.

또한 악의적인 사용자가 주변 환경 속에 설치돼있는 IoT 서비스에서의 단말, 센서와 RFID에 접근하여 데이터를 수집하거나, 단말 자체를 파괴 할 가능성도 있다.

3.1.2 네트워크

스마트폰에서 사용하는 대표적인 네트워크 기술로는 2G/3G/LTE, WiFi, Bluetooth, NFC 등이 있다. 네트워크에서의 보안 위협은 일반 무선통신환경에서 발생할 수 있는 문제점들과 같다. 비인가 사용자의 접근, 불법 Access Point, 패킷 스니핑, ARP 스푸핑 공격 등으로 정보를 도청/유출 당할 수 있다. 또한 IoT 서비스는 많은 수의 노드들이 통신하기 때문에 서비스 거부 공격으로 인해 네트워크가 마비될 위험도 존재한다.

3.1.3 플랫폼

플랫폼의 취약점을 이용한 공격위험이 있다. 모바일 OS는 대표적으로 ios와 안드로이드가 있고, 이 두 OS는 키보드 해킹, 바이러스 등의 취약점을 가지고 있다. 또한 사용자가 쉽게 임의로 펌웨어를 변조시키는 루팅, 탈옥이 가능하다. 루팅은 안드로이드의 경우이고, 탈옥은 ios에 해당한다. 이러한 잘못된 접근 제어로 정보 유출의 위험이 있다.

4. 스마트폰을 활용한 IoT 서비스에서의 보안 요구사항

4.1 단말

단말기의 도난, 분실이 발생하면 단말에 저장된 연락처, 문자 또는 SNS, 사진 등 개인정보가 고스란히 노출된다. 또한 비인가 사용자의 IoT 서비스 접근이 가능하여 스마트폰을 이용한 위/변조로 인해 부작용이나 위험을 초래할 수 있다. 이와 같은 위험을 막기 위해 단말 자체에 대한 잠금장치가 요구된다. 현재 대부분의 스마트폰은 PIN과 패턴 잠금을 통해 잠금 기능을 제공하고 있다. 최근에 사람의 신체를 보안 기술에 접목시킨 생체보안이 단말에 적용되고 있는 추세이다. 생체보안은 사람이 가진 고유한 특성을 이용하여 다른 보안방식보다 안전성을 추구한다. 생체보안이 적용된 스마트폰의 사례는 아래와 같다.

• 삼성전자

- 삼성전자는 홍채인식 기술을 탑재한 스마트폰을 개발하고 있다. 2012년도에 '홍채 인식 및 근접 센싱 가능한 단말 장치 및 방법'이라는 이름의 특허(출원번호 10-2012-0047311)를 출원한 상태이다.

• 애플

- 애플은 2013년 가을 '터치아이디' 기능을 추가한 아이폰 5S를 출시하였다. 터치아이디는 홈 버튼을 통해 지문을 인식하여 등록된 사용자가 맞는지 아닌지를 판단한다. 사용자는 홈 버튼을 누르기만 하면 된다.

• 팬택
- 팬택이 2013년 10월 출시한 '시크릿노트'는 스마트폰 뒷면에 지문인식 장치를 탑재하고 있다. 사용자는 뒷면의 장치를 손가락으로 문지르듯이 쓸어내리면 된다. 팬택은 홈 화면 잠금 해제 기능 외에 시크릿모드를 추가하여 개인적인 콘텐츠를 숨기고 지문인식을 통해 잠금 해제 하는 기능을 제공한다.

또한 도난, 분실된 스마트폰을 원격제어 하여 저장된 정보를 안전하게 삭제할 수 있어야 한다.
센서와 RFID 자체를 보호하기 위해서는 안전한 암호화와 프로토콜이 사용되어야 한다.

4.2 네트워크

공격자는 스마트폰을 악성코드에 감염시키고 그 후에 네트워크를 이용하여 정보를 위/변조, 유출시키는 경우가 많다. IoT는 연결을 기반으로 하는 것이므로 유무선 통신 프로토콜 자체의 보안취약점을 개선해 나가는 것이 필요하다. 또한 잘못된 접근을 제한할 수 있도록 AP의 강화된 보안 암호 설정 및 인증 기술개발이 요구된다.

4.3 애플리케이션

스마트폰을 활용한 IoT 서비스는 개방성이 크다. 개방성이 큰 만큼 사용자 인증 및 강력한 접근제어 기술이 요구된다. 개방형 애플리케이션 서비스의 경우 마켓에 올라가기 전 악성 애플리케이션 여부를 판단할 수 있도록 해야 할 것이다. 또한 애플리케이션으로 전송된 데이터의 무결성을 보장할 수 있는 암호화 등의 메커니즘 적용이 필요하다.

4.4 정보 보호

IoT 서비스를 위해서 다양한 센서, RFID를 통해 정보를 수집한다. 정보 수집 시 센싱 대상 정보, 사용용도, 정보 활용 기한 등을 정보 주체에 명시하고 동의를 얻어야 한다.[3] 개인정보의 저장, 전송 시에 암호화와 접근/권한 제어로 개인정보 유출을 방지해야 한다.

5. 결론

본 논문에서는 IoT 기술과 스마트폰에서의 IoT 서비스에 대한 보안 위협을 알아보았다. 그리고 이러한 보안 위협에 대한 보안 요구사항을 제시하였다. 사용자에게 접근성이 좋은 스마트폰을 활용한 IoT 서비스가 쉽고 안전하게 이루어지기 위해서는 IoT 특징에 맞는 보안의 취약점 분석과 대응방법에 대한 연구가 진행되어야 할 것이다.

참고문헌

[1] Tae-shik Shon, Jong-bin Ko, "A Trend of Security of IoT Based on Cloud Computing"

[2] Ho-won Kim, Dong-kyue Kim, "An IoT technology and security"

[3] Hwa-jung Seo, Jong-seok Choi, Dong-geon Lee, Ho-won Kim, "A Trend of Security Technology of IoT"