사물인터넷 융합 서비스 보안 요구사항

강남희
덕성여자대학교

요 약

최근 다양한 산업 군에서 ICT 융합 서비스가 활발히 개발되고 있고 사물인터넷(IoT: Internet of Things) 기술이 신성장 동력의 핵심 기술로 주목받고 있다. IoT는 기존에 연결을 고려하지 않았던 생활 속 모든 것들을(daily life objects) 상호 연결시켜주는 기술이다. 가트너는 현재 1% 미만의 사물만이 인터넷에 연결된 상황으로 보고하고 있고 Cisco의 자료에 따르면 2020년에는 연결된 장치 수가 500억 개 이상으로 증가할 것으로 예측하고 있다. 많은 장치가 연결되는 IoT 환경에는 많은 취약점과 보안 위협이 존재할 것이므로 보안과 개인정보 보호 기술은 반드시 제공되어야 하는 핵심기술이다. 본고에서는 IoT 기반 융합 서비스에서 발생했던 침해 사례를 살펴보고, 안전한 서비스 개발을 위한 기본적인 보안 요구사항을 제시한다.

Ⅰ. 서 론

사물인터넷 (IoT) 기술은 사람과 장치 간 통신 기술 및 데이터 취득을 위한 센싱 기술은 물론이고, 가상의 프로세스, 공간, 동/식물, 저장 데이터 등 모든 것들이 인터넷으로 연결되어 정보가 생성 · 수집 · 공유 · 가공 · 활용되는 지능형 서비스 플랫폼을 포함한 기술이라고 할 수 있다. 다양한 융합 서비스를 개발하기 위한 IoT 서비스 플랫폼 기술은 다양한 버티컬 서비스 단위의 독자적 구현보다 하나의 공통된 형태로 제공될 것으로 예측된다[1].

공통 플랫폼은 애플리케이션과 플랫폼의 개발 비용을 줄이고, 이종의 디바이스들 간의 상호호환성 제공, 사물 인터넷 서비스 융합을 통한 부가가치 창출 등에 장점을 갖는다. 이러한 이유로 국내외 대형 ICT 기업들은 IoT 기술을 플랫폼 사업과 통신 인프라 사업 관점에서 접근하고 있지만 사용자가 체감할 수 있는 응용 서비스는 여전히 부각되고 있지 않다. 주요 가전사를 중심으로 활발히 개발되고 있는 스마트 홈, 스마트 오피스 정도가 사용자들에게 소개되고 있는 정도이다. 향후 사물인터넷 기반 인프라와 플랫폼이 확장되고 시장의 규모가 커질수록 다양한 응용과 서비스에 IoT 기술이 적용될 것으로 예측된다. IoT 세계 시장은 2011년 26.82조원에서 2015년 47.07조원으로, 국내시장은 2011년 4,147억원에서 2015년 13,474억원으로 성장할 전망 되고 있다[2].

기존의 ICT 기술이 유관 산학연을 중심으로 연구 개발되어 왔다면, IoT 기술은 다양한 융합 서비스 관점에서 접근되고 있다. 금융, 의료, 농수산 유관 산업, 제조 공장 등 전통적인 비 ICT 산업들에서 IoT 기술을 적용한 융합 서비스들을 활발하게 연구하고 있다. IoT 플랫폼 기술의 융합을 통해 새로운 개념의 융합 서비스 시장이 창출될 것으로 기대된다. 일예로 국내의 경우 최근 핀테크(FinTech)라는 신규 금융 서비스에 많은 관심이 모아지고 있다.

금융(financial)과 ICT 기술(Technique)을 합성한 핀테크는 ICT 기반 융합 금융 서비스로 모바일 송금과 빠른 결재 등을 필두로 개인자산관리 및 펀딩 등 다양한 금융 서비스로 확장되고 있다. 핀테크가 관심을 받기 전에도 금융 산업에서는 IT 시스템의 고속 연산 능력과 정보 저장 기술을 주로 활용해 인터넷 뱅킹, 주식 거래 프로그램, 인터넷 쇼핑 결제 시스템 등 다양한 금융 서비스를 제공해 왔다. 그러나 모바일과 스마트 기기 활성화

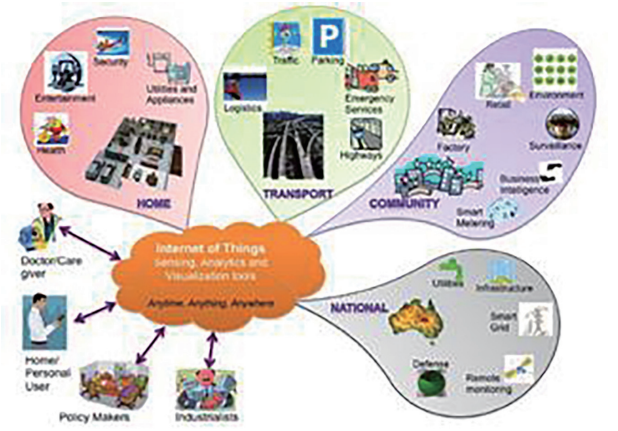


그림 1. 다양한 IoT 융합 서비스 영역[3]

로 ICT 환경이 변화되면서 금융기관 중심으로 ICT 기술을 활용하던 방식에서 비금융 IT 업체를 중심으로 빠르고 저비용인 금융 서비스를 개발하는 방향으로 발전하는 특징을 보이고 있다.

핀테크 기술은 기존의 금융 서비스와 달리 금융 상품 자체의 개발보다 시간과 장소에 제한받지 않는 접속 가능성과 사용자의 편의성에 ICT 기술을 활용하고 있다. 또한 운영하고 있는 ICT 플랫폼의 많은 사용자를 최대한 활용해 결제 대행이나 대출에서 저가의 금융 상품을 제공할 수 있고, 누적된 기존 사용자의 정보를 활용한 빅데이터 기반 금융 분석 서비스 등 신규 서비스를 제공할 수 있다.

본고에서는 다양한 산업에서 진행되고 있는 IoT 기반 융합 서비스에서 반드시 고려해야하는 보안 요구사항을 살펴본다. 이종의 유무형 사물들이 상호 연결되어 정보를 교류하게 되는 IoT 환경에서 정보보안 기술 및 보안 요구사항의 이해는 중요한 요소이다.

본고의 구성은 다음과 같다. 2장에서 IoT 융합 서비스에서 발생할 수 있는 보안 위협을 살펴본다. 이를 기반으로 3장에서 IoT 제품과 서비스가 개발되고, 각 서비스에 적용되어 운영될 때 고려해야 하는 보안의 기본 가이드라인을 제시하고 4장에서 결론을 맺는다.

Ⅱ. 융합 서비스 보안 취약성

일상의 사물에 IoT 기술을 적용할 경우 인터넷을 통해 정보를 주고받는 장치의 수는 대폭 증가한다. 사물의 연결을 기반으로 서비스되는 스마트 홈, 스마트 카, 스마트 공장 등 다양한 스마트 서비스로 사용자의 생활은 편리해 질 수 있지만 인터넷을 통한 공격의 대상이 크게 증가하고 이를 통해 유출되는 정보를 이용하는 2차 보안 위협 역시 증가하게 된다. 보안 전문사인 안랩의 보고 자료에 따르면 2014년 안드로이드 기반 스마트폰을 대상으로 하는 악성코드 수가 2012년 대비 5.4배로 증가하여 총 143만개 이상으로 조사되었다. 또한 간편결재를 중심으로 활성화되고 있는 모바일 핀테크 서비스를 대상으로 하는 새로운 위협들이 해외에서 등장하고 있고 국내에서도 모바일 앱카드의 도용이 발생한 바 있다[5]. 본 장에서는 다양한 융합 서비스에서 발생했던 위협 사례를 살펴본다.

1. 스마트 가전의 위협사례

최근 다양한 기기들이 적용되어 스마트 가전 및 스마트 홈 서비스에서 많은 보안 취약점들이 보고되고 있다[6]. 미국 네트트사에서 판매하는 온도조절 장치의 경우 전력을 효율적으로 사

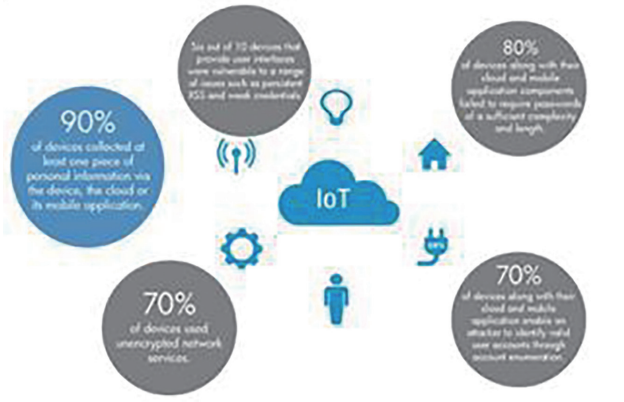


그림 2. IoT 보안 취약성 (HP Fortify 보고)

용하기 위해 댁내에 움직임을 판단해 온도를 자동 조절하는 기능이 있다. 이러한 정보들이 보안 기능의 부재로 유출된다면 개인의 사생활 침해는 물론 물리적 침입까지 유도될 수 있다. 실례로 2014년 블랙햇 컨퍼런스에서 이 장치의 USB 포트를 이용하여 장치 내 메모리에 코드를 주입하고 실행하는 시연이 있었다. 즉, 장치에 백도어 멀웨어 심기 및 펌웨어 해킹이 가능하다. 이를 포함하여 다양한 위협 사례들이 보고되고 있다[7].

- Proofpoint사의 보고에 따르면, 2013년 말부터 2014년 초 10만 대 이상의 스마트 TV, 스마트 냉장고, 라우터 등 가정용 장비에 감염된 Thingbots을 통해 총 750,000건 이상의 피싱과 스팸 메일이 발송되었음
- 리눅스 달로즈 웜으로 PHP 취약점을 악용하여 보안용 IP 카메라, 셋톱박스, 무선랜카드 등 리눅스 OS를 사용하는 IoT 기기들 감염되었음
- FOSCAM 제품의 취약점 이용 유아 모니터링 카메라를 해킹
- 집안, 카페, 주유소 등에 설치된 카메라의 보안 취약 (2014년 채널A 취재결과 1123개의 장소에 설치된 6000여 CCTV중 498곳의 3천29대가 화면 노출)
- 2013년 국내 방송(MBC)에 따르면 전국에 설치된 CCTV는 396만대, 현대인들은 하루 평균 83번 CCTV에 노출된다는 통계 (이 중 88%는 민간 CCTV로 보안에 취약함)
- 2014년 미국 감시 카메라와 유아 모니터를 통해 700여 대의 카메라에서 전송된 실시간 영상 링크를 인터넷에 유포한 사례
- Hack in the Box 보안컨퍼런스에서 무선 IP카메라의 펌웨어 변형공격 시연
- IP 카메라의 경우 보통 80여개 정도의 HTTP 세션만을 설정할 수 있어, DoS 공격을 통해 모든 IP 카메라 기능 정지 가능(일상에 사용되는 소형 기기의 경우 RAM의 제한으로 DoS 공격에 취약함)

2. 스마트 카의 위협사례

자동차를 포함한 교통 시스템의 경우 해킹으로 인한 오작동은 사고로 이어질 수 있어 의료 융합 서비스에서처럼 보안 기능은 반드시 제공되어야 한다. IoT 기술과 자동차가 융합되기 전 자동차 해킹은 물리 접근 공격에 의존했지만 인터넷과의 연결성이 제공되는 스마트 카의 경우는 원격 제어가 가능하다[15].

스마트 카 보안에 대한 위협 사례가 많이 보고되고 있음에도 아직 대응 기술은 초기 연구 단계이다. 최근 크라이슬러사는 원격 해킹의 위험(UConnect 정보엔터테인먼트 시스템의 취약점)을 인식해 자동차 140만대를 리콜했다. 보고된 취약점을 이용하면 운전 중이던 차의 조작은 물론 시동도 끌 수 있다. 이는 보안 기능의 부재가 단순한 정보 유출만의 문제가 아님을 제조사는 인식해야한다. 이 이외의 취약점 보고 사례는 다음과 같다[7][15].

- 2013 블랙햇 컨퍼런스에서 자동차의 디지털 콤파스, 휠 인코더, 관성 측정 유닛 등의 센서에 잘못된 정보를 흘려 급정거하거나 차선을 이탈 등 조작 시연
- 2013년 데프콘에서 포드 이스케이프와 도요타 프리우스에 대해 CAN과 전장 ECU 해킹 코드 공개 및 시연
- 2012년 미국 데이터 암호화 및 인증 절차의 부재로 고속도로 교통표시판(VMS) 및 교통 제어 시스템이 해킹됨
- 2012년 OBD-Ⅱ(자기진단장치)의 취약점 이용 리모콘 열쇠 복제(영국에서 복제 열쇠로 BMW 차량 300대 이상이 도난당한 사건 발생)
- 2011년 USENIX 컨퍼런스에서 자동차의 텔레매틱스 장비를 해킹하여 차량을 제어하는 시연
- 2010년 원격에서 자동차의 도난 방지 기능을 해킹한 사례(미국 텍사스에서 100대 이상의 자동차가 시동에 걸리지 않거나, 지속적으로 경적을 울리는 사건 발생)

3. 의료 ICT 융합 서비스의 위협사례

의료 및 헬스케어 서비스에서도 ICT를 융합한 서비스들이 개발되고 있고 다양한 의료 장치(IMD: Implantable Medical Devices)들의 사용이 증가하고 있다. 의료나 헬스케어 서비스의 경우 민감한 의료정보와 개인정보를 기반으로 하므로 보안 기술의 적용과 유관 정책은 반드시 수립되어야 한다. 더 나아가 의료시스템의 악의적 작동은 생명과 직결된 문제로 보안은 선택이 아닌 필수 서비스가 된다. 다음은 의료 ICT 융합 서비스에서 발생했던 위협 사례들이다[7][16].

- 2013년 생화학 자동분석 시스템에 연결된 오라클 데이터베이스의 취약점을 이용한 해킹으로 원격에서 DB에 오류 정보를 삽입할 수 있음이 보고

그림 3. IoT 장치의 해킹 사례 (Philips Hue, 심박조율기)

- 2013년, 2014년 국내의 의료정보 대량 유출 사건 (2013년에는 의료정보 기록에 접근 가능한 EMR 인증서기 유출되었고, 2014년능 진료 및 처방 기록들이 홍콩에 있는 서버에 송신되었음)
- ATM기기 해킹 시연으로 유명해진 버나비 잭은 심박조율기(pacemaker)를 해킹하여 사망에 이르게 할 수 있다고 주장(인공심장박동기의 해킹 가능성은 2008년 논문으로도 발표되기도 했음)
- 2013 블랙햇 컨퍼런스에서 보안업체 인가디언스는 무선 인터넷과 인슐린 펌프를 해킹하여 당뇨 환자에게 약물을 과다 투여하는 방식을 시연 (2015년 미국은 해킹에 취약한 인슐린 펌프 기의 판매를 제한하고 있음)
- 2013년 미국 FDA는 네트워크에 연결된 의료기기를 대상으로 하는 악성 코드 감염된 사례를 발표함 (환자의 정보 및 모니터 시스템, 임플란트 장비에 무선으로 연결되는 모바일 기기 겨냥)
- 2012년 ICS-CERT Monthly Monitor는 의료기기의 원격 모니터링에 대한 경고 발표 (네트워크 취약점을 이용한 접근)

4. 핀테크의 보안 이슈

모바일을 중심으로 서비스되고 있는 핀테크 기술은 사용자의 편의성과 빠른 처리를 중시한다. 따라서 편리하면서도 강한 보안을 제공해야 한다는 어려움이 있다. 핀테크 기술의 선도 역할을 수행하고 있는 페이팔의 경우 수년 전부터 크로스사이트 요청위조(CSRF) 취약점 등을 이용하여 계정이 탈취될 수 있고, 해킹된 계정을 판매하는 전문 사이트들이 있다고 보고되고 있다. 핀테크 제공 업체는 개인 정보 유출은 물론 기존 금융 업체와 동등한 신뢰성을 확보하기 위한 다양한 노력을 수행해야 한다. 미국 양키그룹의 451 리서치에 따르면 신용카드를 모바일 결제로 대체하기 꺼려지는 가장 큰 이유가 보안이라고 최근 보고되고 있다(응답의 84%). 국내의 경우 아직 서비스가 개화되기 전이라 큰 침해 사례가 보고되고 있지 않지만 금융의 특성으로 공격자의 주 대상이 될 것임은 쉽게 예측할 수 있다. 금융 서비스를 포함한 다양한 위협 사례는 다음과 같다[17].

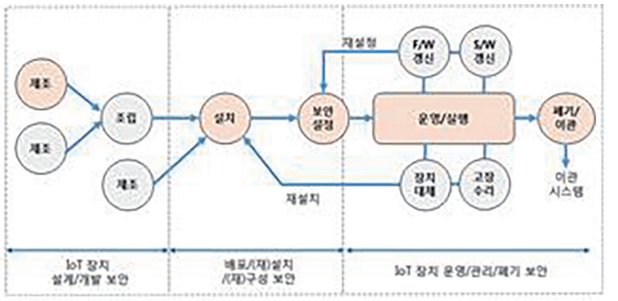
- 편의성을 강조하는 핀테크의 특성 상 사용자 인증의 단순성을 보조하기 위한 부가 인증 기술 (지문인식, 패턴인식 등)이 사용되는데 모바일 기기의 취약성이나 증가하는 악성코드에 대처할 수 있는 방안이 미비하여 ID 도용, 인증 우회, 사회공학적 공격 등이 가능함
- 핀테크 서비스는 기존 금융 서비스와 PG사 및 ICT 회사가 연계되어 서비스를 진행하게 되므로 보안의 통합 설정이 어렵고 각 사의 연결 구간에서 세션 하이재킹이나 DoS 공격이 가능함
- 금융에 필요한 정보(카드정보, 은행 계좌 정보 등)를 관리하는 주체가 금융회사에서 PG사, 온라인 플랫폼 제공사 등으로 확대될 수 있지만, 서비스 초기에는 정보 관리 및 정보 공유 절차의 안전성 확보가 부족함 (2013년 미국 타켓사의 1억건 이상의 개인 정보 유출 사고처럼 연계되어있는 서비스 체인에서 가장 보안이 취약한 계약 업체가 공격되고 이후 보안이 강한 회사가 공격되는 사례가 있음)
- 핀테크는 초기 인증 이후 거래시 간편한 인증의 편리성에 중점을 두고, 이를 보완하기 위해 지문이나 정맥 정보를 활용한 바이오 인증을 수행하고 있음; 이 경우 인증기법의 취약점을 이용한 ID 도용, 추가인증 우회, 피싱 및 파밍 공격 등의 보안 위협이 존재함

Ⅲ. 사물인터넷 공통 보안 원칙

사물인터넷 기반 융합 서비스의 활성화를 위해 보안은 필수 기술로 인식되고 있다. 3장에서 기술했듯 다양한 융합 서비스에서 보안이 제공되지 않을 경우 정보 유출이나 단순한 경제적 피해는 물론 서비스에 따라 생명을 위협할 수 있기 때문이다. 또한 비 ICT 산업에서 사용되는 다양한 이종 기기들이 인터넷을 주 매체로 정보를 주고받는다는 것은 공격의 대상 및 범위의 증가를 의미하고, 침해 시 피해 규모는 상상 이상일 것으로 예측된다.

이러한 인식을 기반으로 미래창조과학부는 2015년 6월 산학연으로 구성된 사물인터넷 민간 협의체로 '사물인터넷보안 얼라이언스'를 출범하고 사물인터넷 제품 및 서비스를 위한 7대 공통 보안원칙을 공표했다[8]. 본 장에서는 사물인터넷 기기 및 서비스의 전주기를 고려해 공표된 보안 원칙을 기술한다.

공통 보안 원칙의 기본은 IoT 장치 및 서비스의 설계에서 운영까지 전주기를 고려하여 보안의 잠재적 위협요소와 취약점을 점검하고 보완하는데 중점을 두고 있다. 다음 그림은 IoT 융합 서비스를 구성하는 기기와 서비스의 전주기 단계를 나타낸다.



※ F/W: Firmware, S/W : Software

그림 4. IoT 장치의 전주기 단계별 보안

1. 설계/개발 단계

IoT 제조사와 서비스 제공자는 안전한 IoT 제품 개발 및 서비스 이용환경을 조성하기 위해 해당 서비스에 대해 정확히 이해하고, IoT 제품과 서비스의 설계 단계에서부터 제품 및 서비스가 적용될 환경을 기반으로 보안 취약점을 사전에 분석하여 이를 보완하고 강화할 수 있는 기술을 적용해야한다. 설계 시 고려해야 하는 공통 보안 요구사항은 다음과 같다.

① 정보보호와 프라이버시 강화를 고려한 IoT 제품 · 서비스 설계 – 'Security by Design' 및 'Privacy by Design' 원칙 준수
② 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증 (시큐어 코딩, 소프트웨어, 어플리케이션 보안성 검증 및 시큐어 하드웨어 장치 활용)

Security by Design'은 IoT 제품 및 서비스의 설계 단계부터 보안을 내재화하고, 지속적인 대응을 수행하여 서비스 사용자 및 사업자의 자원 및 정보를 보호한다는 개념이다. 또한, Privacy by Design은 IoT 제품 및 서비스의 설계 단계에서 프라이버시 침해 위협을 지속 점검하여 침해가 발생하기 전에 선제 대응하겠다는 프라이버시 보호 개념이다[9].

보안을 고려하지 않고 구현한 프로그램에는 다양한 보안취약점들이 발생할 수 있으며, 이는 IoT 기기와 서비스에 심각한 오

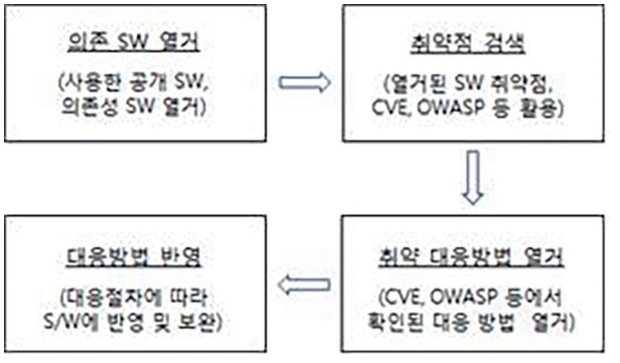


그림 5. SW 보안성 검증 단계

동작, 결함을 야기할 수 있고 잠재되어있는 위험 요소는 공격자의 주요 대상이 된다[10]. Java, C/C++로 개발된 소프트웨어는 현재 마련되어있는 시큐어 코딩 가이드를 활용하고[11][12], 가이드가 개발되어있지 않은 언어는 국제표준에 근거하여 별도의 분석도구 및 방법론을 이용하여 소스 코드에 대한 보안 품질 검증을 수행해야 한다[14].

2. 배포/설치(재설치)/구성(재구성) 단계

IoT 융합 서비스에서 필요한 IoT 장치를 배포하고, 서비스 영역에 설치(재설치) 및 구성(재구성) 할 때 필요한 보안 요구사항은 다음과 같다.

③ 안전한 초기 보안 설정 방안 제공(Security by Default 기본 원칙 준수)

④ 보안 프로토콜 준수 및 안전한 파라미터 설정(통신 및 플랫폼에서 검증된 보안 프로토콜 사용: 암호/인증/인가 기술 포함)

IoT 서비스에 특화되어 제작되는 주변의 사물들은 설정을 위한 사용자 인터페이스가 부재된 경우가 많고, 보안 설정을 일반 사용자가 세밀히 관리하기는 어렵다. 또한 제조시 기본 설정된 계정과 패스워드는 주 공격대상이 되기도 한다. 따라서 IoT 장치의 설치자나 서비스 관리자는 초기 설치 단계와 고장 수리 후 재설치 단계에서 보안 프로토콜들에 기본으로 설정되는 파라미터 값이 가장 안전한 설정이 될 수 있도록 “Security by Default” 기본 원칙을 준수해야 한다.

최근 다양한 국내외 표준 기구 및 사설 표준 기구에서 사물인터넷 관련 보안 기술들을 논의하고 있다[1][13]. IoT 제품 개발자와 서비스 제공자는 데이터 통신 및 개방형 플랫폼에 안전성을 보장하는 검증된 보안 프로토콜을 적용해야 하고, 보안 서비스(암호/인증/인가/가용성 등) 제공 시 안전한 파라미터들이 설정될 수 있도록 해야 한다. 특히, 경량 장치들 간 및 경량 장치와 플랫폼 간의 정보 공유 시 적용 환경을 고려한 경량화 보안 프로토콜의 사용이 고려되어야 한다.

3. 운영/관리/폐기 단계

IoT 서비스과 운영될 때 다양한 보안 위협과 사전에 알려지지 않은 취약점이 존재할 수 있다. 이에 대응하기 위해 다음의 보안기능이 요구된다.

⑤ IoT 제품 · 서비스의 취약점 보안패치 및 업데이트 지속 이행(S/W와 H/W의 보안 취약점에 대해 모니터링하고 업데이트 지속 수행)

⑥ 안전한 운영 · 관리를 위한 정보보호 및 프라이버시 관리체계 마련(사용자 정보 취득–사용–폐기의 전주기 정보의 보호 및 프라이버시 관리)

⑦ IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련(보안사고에 대비한 침입탐지와 사고 시 분석 및 책임추적성 확보)

IoT 제품 제조사와 서비스 제공자는 지속적으로 보안 취약점을 분석하고, 발견 시 보안패치를 신속히 배포할 수 있도록 사후조치 방안을 마련해야한다.

지능화된 IoT 장치가 사용자의 상황 정보를 취득하고 IoT 플랫폼에서 가공된 정보를 기반으로 다양한 서비스가 지원될 것이다. 따라서 다량의 개인정보가 수집 · 저장 · 전송될 수 있으며, 개인정보가 유출될 경우 심각한 프라이버시 침해 문제가 발생할 수 있다. 서비스 제공자는 최소한의 개인정보만 수집 · 활용될 수 있도록 개인정보보호정책을 수립해야한다. 개인정보보호정책 수립 시에는 빅데이터 분석과정에서 특정 개인을 식별할 수 있는 새로운 개인정보가 생성 · 유통될 수 있기 때문에 이를 적절히 통제할 수 있는 기술적 · 관리적 보호조치도 포함되어야 한다.

서비스 제공자는 공격이나 침해 사고가 발생된 후 원인분석과 책임 추적성을 확보하기 위해 로그기록을 안전하게 저장하고 관리해야 한다. 저전력 경량 장치의 경우 자원 제한적인 속성으로 인해 로그기록의 생성과 보관이 어려울 수 있다. 이런 경우에는 서비스 운영 및 관리시스템에서 IoT 장치의 상태정보를 저장하고 관리하는 역할을 대행해야 한다.

Ⅳ. 결 론

본고에서는 IoT 기반 융합서비스의 보안 취약점과 안전한 서비스 개발을 위해 고려해야 하는 보안 요구사항을 살펴봤다. 국내외에서 IoT 기반 융합 서비스를 발굴하여 신규 시장을 개척하려는 다양한 시도가 진행되고 있으나 IoT 보안에 관한 고려는 미비한 상황이다. IoT 보안은 개인 정보의 노출에서 멈추지 않고 생명과 직결되는 제어 메시지가 포함될 수 있어 보안 기술의 적용은 필수적이라 할 수 있다. 본고에서 기술한 공통 보안 요구사항을 기초로 안전한 융합 서비스가 개발되길 기대한다.

Acknowledgment

본 연구는 2015년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2014R1A1A2056961).

참 고 문 헌

[1] 송재승, "초연결 사회를 위한 OneM2M 표준화 기술 동향," TTA Journal, Vol.150, pp.84-89, 2013.11.

[2] 장원규, 이성협 "국내외 사물인터넷 정책 및 시장동향과 주요 서비스 사례," 동향과 전망: 방송 · 통신 · 전파 통권 제64호, 한국방송통신전파진흥원, 2013.06.

[3] Jayavardhana Gubbia, et. al., "Internet of Things (IoT): A vision, architectural elements, and future directions,"Future Generation Computer Systems, Vol. 29, Is. 7, pp. 1645-1660, Elsevier, 2013.09.

[4] 정준호, 김정숙, "핀테크(FinTech) 서비스의 주요 사례와 보안 이슈,"Vol.19(1), pp. 9-15, 한국멀티미디어학회지, Mar. 2015,

[5] 안랩, "2015 모바일 보안위협 예상 트렌드 Big 4,"2015.06. (http://asec.ahnlab.com/1018).

[6] Mario Ballano Barcena, Candid Wueest, "Insecurity in the Internet of Things," Security Response, Symantec, 2015.03.

[7] 강남희, et. al., "IoT 제품 및 서비스 보안성 강화방안 연구," KISA-WP-2015-0020, 한국인터넷진흥원, 2015.09.

[8] 한국인터넷진흥원"IoT 공통 보안 원칙 v1.0,"사물인터넷 보안 얼라이언스, 2015.06.

[9] Information and Privacy Commissioner, Privacy and Security by Design: An Enterprise Architecture Approach, (캐나다 백서)

[10] Security Considerations in the IP-based Internet of Things, IETF(Internet Engineering Task Force), (http://www.ietf.org)

[11] 시큐어코딩(C, Java) 가이드, 행자부, 2014.

[12] OWASP 시큐어 코딩 규칙 참고 가이드, OWASP Korea 챕터, 2011년.

[13] 강남희, "사물인터넷 보안을 위한 표준기술 동향," 한국통신학회지(정보와통신) 31(9), 2014.

[14] ISO/IEC, ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security

[15] 곽병일, et. al., "IoT 관점에서의 차량 위협 탐지 방안," 정보보호학회논문지, Vol. 25(2), pp. 411-421, 2015.04.

[16] 최성호, 곽진, "국외 의료기기 보안위협 사례 및 보안 동향 조사,"정보보호학회지 Vol. 25(3), pp. 11-18, 2015.06.

[17] 박정국, "핀테크(Fintech)와 정보보안," 정보과학회지, Vol. 33(5), pp. 23-32, 2015.05.

약 력

강 남 희

1999년 숭실대학교 공학사
2001년 숭실대학교 공학석사
2004년 Siegen대학교(독) 공학박사
2009년~현재 덕성여자대학교 디지털미디어학과 조교수
관심분야: 유무선 네트워크(QoS, Mobility), 시스템/인터넷 보안