편집위원 : 위 규 진 (한국정보통신기술협회)

IoT(Internet of Things) 정보보호 기술 개발 방향

원 유 재
정보통신기술진흥센터, 충남대학교

요 약

기존의 사이버 환경의 보안 기술은 단순히 데이터, 네트워크, 시스템을 보호함으로써 인간의 자산을 보호하는 차원의 기술이었다면, IoT 환경에서 보안 기술은 궁극적으로 사물들로부터 사람을 보호하는 기술로 패러다임의 변화가 예상된다. 따라서 본고에서는 미래의 새로운 성장동력으로 부상하고 있는 사물인터넷(IoT) 서비스 활성화를 지원하는 동시에 인간의 자산과 생명을 보호하기 위하여 정부차원에서 수립한 정보보호 기술 개발 계획을 정리한다. IoT 정보보호 기술은 디바이스, 네트워크, 서비스/플랫폼의 3개 계층으로 나누어 9개 원천기술로 분류하였다.

Ⅰ. 서 론

사람, 사물, 공간, 데이터 등 모든 것이 연결되는 초 연결사회가 도래함에 따라, 사물인터넷(IoT)이 미래의 새로운 경제성장 동력으로 부상하고 있다. 이에 따라 전세계는 사물인터넷이 차세대 핵심산업으로 부상할 것으로 인식하고 경쟁적으로 대책을 세우는데 부심하고 있다. 미국은 사물인터넷을 국가 R&D 우선과제로 지정하고 차세대 IoT 과학기술 공학분야에 150여개 프로젝트에 대한 연구투자를 지원하고 있다. EU는 사물인터넷 활성화를 위해 기본적으로 추진해야 할 실행과제를 명시한 '사물인터넷 액션플랜'을 수립하였다. 중국도 IoT 전반의 국가 핵심기술 개발, 산업화, 표준화 연구 등에 관한 추진방향을 제시한 '사물인터넷 12차 5개년 발전 계획'을 발표하였다.

그러나, 사물인터넷은 우리 실생활의 모든 사물에까지 직접 접목되기 때문에 기존의 정보 유출 및 금전 탈취 등을 넘어 국가 기반시설까지 심각하게 위협하며, 이로 인한 경제적인 피해가 막대할 것으로 예상되고 있다. IoT 보안위협은 기계 장치의 급발진, 급정지, 오동작 등 사람의 생명을 위협할 만큼 치명적이고, 도입 후에는 사후 보안조치가 불가능하거나 고비용이 수반될 수 있으며, 보안이 적용되지 않은 IoT 제품이나 서비스는 글로벌 시장에서 경쟁력을 상실하게 될 것이다. 따라서 누구나 안전하게 사물인터넷의 편리함을 누리고 이를 창조경제 실현을 위한 미래 신 성장동력으로 활용하기 위해서는 정보보호가 담보된 안전한 IoT 이용환경 조성이 우선적인 과제가 될 것이다.

IoT 환경은 정보보호에도 많은 변화를 가져올 전망이다. 스마트 홈, 스마트 의료, 스마트 카 등 IoT 서비스가 일상생활로 확산되면서 기존 사이버세계의 위험이 현실 세계로 전이 확대될 것이다. IoT 환경은 기존 PC나 모바일 기기 중심의 사이버 환경과 달리 보호대상, 주체, 방법 등에 있어서 새로운 접근을 필요로 할 것이다. 첫째는 모든 사물간 상호연결이 심화되면서 이에 따른 보안 위협 역시 크게 증가 하므로, 제품이나 서비스의 기획, 설계 단계부터 정보보호를 고려해야 한다. 둘째는 보호해야 할 기기의 수가 우리 일상생활의 모든 사물로 확대되고 그 특성도 다양화 되면서 기존의 보안 기술 적용에 많은 한계가 있을 것이다. 셋째는 다양한 분야에 IoT 응용서비스가 도입, 적용되면서 기존 제조업, 서비스업 등 정보보호를 고려치 않아도 되었던 전 산업분야에서도 정보보호를 무시할 수 없게 될 것이다. 〈표 1〉은 보호 대상, 보안 주체, 보호 방법 등의 측면에서 보안 특성이 IoT 환경 이전과 어떻게 달라지는지를 보여 주고 있다.

표 1. 보안 특성의 변화

구 분	As-Is	To-Be
보호 대상	PC, 모바일 기기	가전, 자동차, 의료기기 등 우리 주변 모든 사물(Things)
대상의 특성	고성능, 고가용성을 가지는 운영환경	고성능, 고가용성 + 초경량, 저전력
보안 주체	ISP, 보안 전문업체, 이용자	ISP, 보안 전문업체, 이용자 + 제조사, 서비스제공자
보호 방법	별도의 보안장비, SW 구현 및 연동	별도의 보안장비, SW 구현 및 연동 + 설계단계부터 사물 내 보안 내재화
피해 범위	정보유출, 금전피해	정보유출, 금전피해 + 시스템 정지, 생명위협

따라서 본 고에서는 IoT 환경의 보안 위협에 대응하기 위하여 국가차원에서 수립한 IoT 정보보호 로드맵을 중심으로 기술 개발 계획에 대하여 살펴보기로 한다. 2장에서는 IoT 보안 위협과 보안 요구사항을 정리하고, 3장에서는 IoT SecureDome프로젝트에서 정의하고 있는 IoT 보안 구조를 설명한다. 4장에서는 2015년 정보보호기술 개발 계획 과제 중에 IoT와 관련된 과제에 대해 요약하고, 5장에서 결론을 맺는다.

Ⅱ. IoT 보안 위협 및 요구사항

작년에 개최된 블랙햇(BlackHat) 2014에서는 자동차, 항공기, 가전, 의료기기 등에 대한 해킹 시연이 다수 진행되었는데 이는 IoT 기기들이 보안 문제가 해결되지 않고는 이용확산이 제한적일 수 있다는 것을 단적으로 보여주는 사례가 되었다.

스마트 카의 경우는 무인주행이 가능한 자동차 의 취약점으로 인하여 해킹으로 교통사고를 유발시킬 수 있음을 보여 주었다. 심장박동기의 전류공급 장치를 조작하여 인명사고를 일으킬 수 있는 가능성도 보였으며, 스마트 TV나 로봇 청소기에 악성코드를 감염시켜서 카메라 원격 조종을 통한 프라이버시 침해가 발생할 수 있음도 이미 많이 알려져 있는 사실이다.

IoT 서비스의 구성요소는 서비스의 특성에 따라 다양하지만 대표적으로 디바이스, 네트워크, 플랫폼(서비스 포함)으로 구별할 수 있다. CPU 성능, 메모리 크기, 소비전력 등의 제약을 갖는 IoT 기기에서는 기존 암호기술을 적용하는데 한계가 있을 수 있으므로, 기기의 성능과 보안 강도를 고려한 경량ㆍ저전력 암호기술을 필요로 한다. 악성코드 감염 및 외부 해킹으로 인한 운영체제를 비롯한 소프트웨어 위변조 방지와 권한이 없는 접근을 차단할 수 있는 기능도 요구된다. 또한, IoT 기기의 탈취ㆍ도난ㆍ해킹 등을 통한 불법복제 및 중요 데이터 유출을 방지하기 위하여 하드웨어적인 기법으로 원천적으로 보호할 수 있는 수단도 필요로 하게 된다.

IoT 환경의 네트워크 구성은 통신 방식(ZigBee, Bluetooth, WiFi 등) 뿐만 아니라 서로 다른 서로 다른 처리 능력 등으로 더욱 복잡할 것이다. 이에 따라 보안 특성(암호, 인증방식 등)이 서로 다른 기기와 센서가 상호 연결된 이종 네트워크를 대상으로 하는 해킹 및 악성코드 공격 등을 탐지하고 차단하기 위한 네트워크 보안 기술이 필요할 것이다. 서로 다른 기능을 수행하는 IoT 기기간 통합 네트워킹에 요구되는 단말 상호간 인증, 보안통신 및 접속제어 기능이 요구되며, 악성코드에 감염된 사물봇에 의한 트래픽 폭증 공격(DDoS)을 방지 하기 위한 네트워크 모니터링 및 관리기술은 PC나 모발 기기에서 보다 훨씬 복잡한 형태의 기술을 요구하게 될 것이다.

플랫폼/서비스에서 보안 요구사항은 기본적으로 서비스에 따라서 종속적인 것과 이와 무관하게 또 다른 플랫폼으로 독립적으로 제공해야 할 것으로 구별될 것이다. IoT 서비스 구성 요소(기기, 사용자, 서비스)간 상호 인증, 접근제어 및 프라이버시(위치, ID, 데이터)를 보호하고 위장 사물, 기능이 변조된 사물 등의 서비스 비인가 접속을 차단 하기 위한 암호, 인증, 키 관리 기술이 요구된다. IoT 환경에서 데이터 수집 분석에 의한 프라이버시 침해(개인식별, 추적)를 방지하기 위한 익명화 기술 등도 IoT 서비스가 현실화되면 매우 중요한 요구사항이 될 것이다. IoT 서비스 특성(홈ㆍ가전, 의료, 교통 등)과 동작환경(임베디드, 웨어러블, 모바일 등)에 특화된 보안 플랫폼과 여러 IoT 서비스가 혼재되어 동작(예: 자동차에서 홈ㆍ가전 및 의료서비스 접속)하는 경우, 비용 효율화를 위해 공통기능과 특화기능을 연계한 통합플랫폼도 새로운 요구사항으로 대두될 전망이다.

디바이스, 네트워크, 플랫폼으로 구별하여 보안 요구사항을 언급하였지만 서비스 운영단계를 중심으로 보면 이들 기능들이 모두 연결되어 동작하게 되므로 상호 연결성과 상호 연동성이 매우 중요하다. 따라서, 제품과 서비스의 설계단계부터 보안을 내재화하고, 체계적인 사이버위협 대응체계 구축 등 IoT 보안 기반을 마련하는 것이 매우 중요하다.

Ⅲ. IoT SecureDome 프로젝트

〈그림 1〉은 IoT 서비스가 동작하는 환경을 디바이스, 네트워크, 서비스/플랫폼 3계층으로 나누고, 각 계층마다 필요한 핵심 원천기술들을 정리하였다. 이것은 기본적으로 디바이스 계층에서의 보안 기술과 네트워크 계층에서의 보안기술, 그리고 서비스/플랫폼 계층에서의 보안 기술을 고려할 수 있다는 것을 나타내며, 서비스에 따라서는 각 계층의 보안 기능들을 필요에 따라서 선택적으로 사용될 수 있음을 나타낸다. 이와 같이 IoT 서비스를 3개 계층으로 나누어 각각을 디바이스 Dome, 네트워크 Dome, 플랫폼/서비스 Dome으로 구별하고, 9개의 원천기술을 개발하는 계획을 IoT SecureDome 프로젝트라 명명하였다.

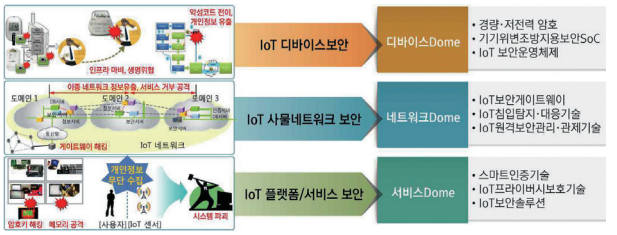

그림 1. IoT 보안 구조

IoT 디바이스 보안(디바이스 Dome)은 IoT 기기(디바이스)의 크기(MCU, 메모리), CPU 성능, 전력소모량 등을 고려한 경량ㆍ저전력 암호 모듈, HW 보안SoC(System on Chip) 및 IoT 보안 운영체제 기술을 포함한다. 암호기술은 단기적으로 기존 암호기술을 경량화 및 저전력화 하고, 중장기적으로 신규 암호 알고리즘을 개발하여 IoT 기기 및 네트워크 플랫폼에 적용할 계

획이다. 하드웨어(HW) 기반의 경량ㆍ저전력 암호 모듈을 개발하여, 신체 부착형 웨어러블 기기 및 초소형 센서 등에 대한 위변조(ID) 및 부채널 공격을 방지하는 보안 SoC를 개발하여 IoT 디바이스에 부품으로 활용되도록 하는 동시에, IoT 디바이스 개발 과정에서 시험환경으로도 활용될 수 있도록 할 계획이다. 보안 운영체제 기술은 기기의 핵심 자원(운영체제, 개인정보 등)에 대한 비인가 접근차단 및 시스템 소프트웨어의 위변조 방지, 경량ㆍ저전력 암호모듈 탑재를 통한 보안 기능 등이 내재된 운영체제(Secure OS) 핵심기술이다. 모듈형 보안 운영체제를 개발하여 스마트의료, 스마트카 등 인간의 안전과 직결되는 IoT 기기의 센서 및 게이트웨이 등에 재구성하여 적용할 계획이다.

IoT 사물네트워크 보안(네크워크Dome)은 이기종 기기가 상호 연결된 사물네트워크 환경에서 실시간 이상징후를 탐지 및 대응하는 보안기술을 포함한다. 보안 게이트웨이 기술은 신뢰/비신뢰 기기 및 이종 네트워크간 상호연결성(Bridge)과 보안 통신을 제공하는 기술이다. IoT 서비스 분야(홈/가전, 의료, 교통 등) 별로 상이하게 요구되는 기기 간 연결 통신 방식(WAVE, IEEE11073, AllJoyn 등) 및 트래픽 특성을 고려한 보안 기능 제공해야 한다. 또한, 기기가 제공하는 통신 방식에 따른 가상화 환경에서 필요한 보안 기술도 여기에 해당된다. IoT 침입탐지 대응기술은 IoT 기기와 네트워크의 물리적/행위적 이상징후를 탐지하여 실시간으로 대응하는 클라우드 기반 IoT 침입탐지 대응 기술을 말한다. IoT 기기에 대한 공격과 오동작 및 결함을 클라우드에서 집단지성을 활용하여 집중적으로 처리, 분석, 판단하여 검출이 가능한 동적 침입방지기술이다. 원격보안관리 기술은 유무선기기의 보안상태를 원격 모니터링 하여 보안SW, 규칙, 정책 등을 자동으로 업데이트(패치)하는데 필요한 기술로서 빅데이터 분석 기반으로 기기의 오동작을 사전 예측하는 기술과 대규모 악성 분산 트래픽 공격을 탐지 대응하는 보안관제 기술이다.

IoT 플랫폼/서비스 보안(서비스Dome)은 웨어러블 등 IoT 서비스 환경에 적합한 인증, 프라이버시 보호 및 IoT 서비스용 보안솔루션 기술을 포함한다. 스마트 인증 기술은 이용자의 생체 정보나 행위 패턴을 이용하여 사용자 인증과 기기의 접근 권한관리 기능을 제공하는 스마트 인증 기술이다. IoT 네트워크 기기간 인증을 위하여 확장 가능한 키분배 기술이나 전통적인 PKI에서 벗어나 IoT 환경에 특화된 경량 PKI 기술이 요구될 수 있다. 프라이버시 보호 기술은 비정형 IoT 빅데이터를 실시간으로 분석하여 민감한 정보 노출 위험을 탐지하거나 제거하는 기술을 포함하며, IoT 디바이스를 통한 이용자 위치 및 이용내역 추적을 방지하기 위해 적용하는 이용자 신원 및 위치정보 은닉 기술 등이 여기에 속한다. IoT 보안 솔루션으로 표기된 기술은 IoT 서비스 분야별 기술특성(프로토콜, 요구표준 등)을 고려한 적응형 IoT 보안 기술을 나타낸다. 스마트홈/가전에서 개인정보 및 프라이버시 보호를 위한 암호화, 스마트카에서 차량용 고속 보안통신, 스마트의료에서 가용성과 실시간성이 보장되는 접근제어 기술 등이 여기에 속한다.

IV. IoT 정보보호 기술개발 과제 요약

〈표 2〉는 2015년 정보보호 기술개발 과제 후보로 기획한 과제들 중에서 IoT 정보보호 기술과 관련된 과제들이다. 표에서 적용 대상은 목표로 하는 과제의 결과물이 적용될 대상이 〈그림 1〉에서와 분류한 바와 같지만, 암호라이브러리가 통신 과정에 적용된다면 디바이스뿐만 아니라 네트워크 또는 서비스에도 적용될 수 있기 때문에 적용대상이 복수인 경우를 나타내기 위해 사용되었다

표 2. 2015 IoT 정보보호 후보 과제

번호	과제명	적용대상
1	다양한 IoT 서비스용 경량 암호/인증 보안 라이브러리 개발	디바이스 /네트워크/서비스
2	IoT 디바이스 보안을 위한 콘트롤러 칩(SoC) 세트 개발	디바이스
3	스마트 경량 IoT 기기용 운영체제 보안 핵심 기술 개발	디바이스/서비스
4	계층적 식별자를 가진 인터넷 개체의 공개키 인증구조 연구	디바이스/서비스
5	멀티팩터 인증 및 전자서명을 제공하는 인증 플랫폼 개발	디바이스/서비스
6	박막 타입 지문센서 모듈 및 프라이버시 보호 기술개발	디바이스/서비스

정리된 후보 과제들은 정해진 예산 범위 내에서 추진되기 때문에 일부만 추진 될 수도 있다. 그럴 경우 디바이스에 적용될 기술들이 다른 기술들에 비해서 우선순위가 높은데, 그 이유는 IoT 디바이스 개발에 신속하게 적용될 수 있도록 하기 위함이다. 특히, 암호/인증 보안 라이브러리는 성능이 중요한 관건이기 때문에 1차년도에 주관기관을 2개 선정하여 성능 평가를 통하여 우수한 기관에게만 2차년도 과제를 추진하도록 하는 경쟁형 과제로 추진할 예정이다. 이렇게 함으로써 IoT 서비스에 최적의 암호/인증 보안 라이브러리가 활용될 수 있는 환경을 만들어 나갈 계획이다.

V. 결론

본고에서는 IoT 보안 기술 개발 방향에 대하여 살펴보았다. 3개 계층의 9개 원천기술로 IoT 보안을 표현한 것은 가장 상위레벨의 분류이다. 따라서, IoT 환경의 모든 보안 위협을 감당하는 기술로 보기에는 현실적으로 부족함이 있고, 그 또한 정해진 예산 범위 내에서 정부과제가 추진되기 때문에 계획한 9개 과제가 모두 추진되기도 힘든 상황이다. 그렇지만 IoT 보안 기술에 대해 디바이스, 네트워크, 서비스/플랫폼으로 계층을 나누어 접근하고, 또 이들에 대해서도 독립적인 솔루션 개발이 가능한 것과 디바이스, 네트워크, 서비스/플랫폼 등과 밀결합 형태로 개발되어야 하는 기술들을 나누어 접근하는 것은 매우 중요한 일로 생각된다. 앞으로 점점 더 보안 기술 들은 개발과정이나 운영과정 모두에서 적용 대상과 밀결합 형태를 보일 것이며, IoT 환경은 디바이스가 갖는 특성상 더욱 그런 특성을 보일 것이다. 이렇게 정리한 결과가 IoT 정보보호 기술에 대한 정부의 기술개발 계획을 이해하는데 도움이 되고, IoT 보안 기술을 개발하는 전문가뿐만 아니라 IoT 서비스를 개발할 계획을 가지고 있는 전문가들 모두에게 조금이라도 도움이 되길 기대한다.

참 고 문 헌

[1] 미래창조과학부, 사물인터넷(IoT) 정보보호 로드맵, 2014. 10.
[2] 미래창조과학부, 사물인터넷(IoT) 기본계획, 2014. 5.
[3] Black Hat 2014, https://www.blackhat.com/us-14/archives.html

약 력

원 유 재

1985년 충남대학교 이학사
1987년 충남대학교 이학석사
1998년 충남대학교 이학박사
1987년~2001년 한국전자통신연구원 무선인터넷정보보호팀장
2001년~2004년 안랩유비웨어 연구소장
2004년~2014년 한국인터넷진흥원 인터넷침해대응센터본부장/경영기획본부장
2014년~현재 충남대학교 컴퓨터공학과 교수
2013년~현재 미래창조과학부 정보보호 CP(IITP 파견)
관심분야: 사이버보안, 이동통신보안