편집위원 : 이임영 (순천향대학교)

초연결 환경에서 보안위협 대응을 위한 사물인터넷(IoT) 보안 기술 연구

김정녀, 진승헌
한국전자통신연구원

요 약

각종 사물에 네트워크 기능이 탑재되어 초연결 통신으로 연결되는 사물인터넷(IoT, Internet of Things) 기술이 급속히 확산됨에 따라, 최근에는 그 사물 자체가 지능화되어 지능형 스마트 사물로 진화하고 있다. 기기들이 자신을 구별할 수 있는 유일한 IP를 보유하면서 사물인터넷에 연결되어, 모든 기기가 해킹의 대상이 될 수 있어 보안적인 측면에서도 취약하게 되었다. 본고에서는 최근들어 급증하는 초연결 네트워크 환경과 사물인터넷에 대하여 알아보고, 초연결 환경에서 보안 위협에 대응하는 사물인터넷 보안 기술에 대한 연구와 표준화 동향, 그리고 사물인터넷 보안 위협에 대응하는 보안 기술의 방향을 알아본다.

Ⅰ. 서 론

최근 각종 사물에 네트워크 기능이 탑재되어 인터넷에 연결되는 기술인 사물인터넷(Internet of Things, 이하 IoT)[1] 기술이 급속이 확산됨에 따라 스마트 홈, 스마트 헬스케어, 스마트 자동차, 스마트 에너지 등 다양한 응용 환경에서 사물이 지능화되어 지능형 스마트 사물로 진화하고 있다.

시장조사기관인 비즈니스 인사이더에 의하면 〈그림 1〉과 같이 사물인터넷의 시장이 급속이 증가하고 있어 전세계 사물인터넷 시장의 규모는 연평균 약 44%의 고성장을 통해 2020년 6,000억 달러에 이를 것으로 전망되며, 특히 소프트웨어 및 서비스 시장의 비중이 높을 것으로 예측되고 있다. 이에 최근 인터넷에 연결된 기기의 대수가 100억대에 이르며, 2020년에는 300억대까지 증가할 것으로 예상한다[6][ABI Research].

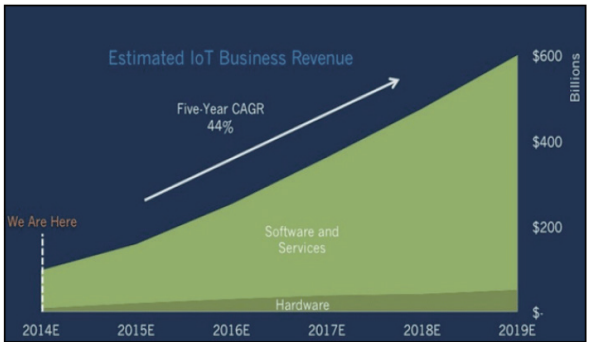

그림 1. 사물인터넷(IoT) 시장

IoT 기기의 보급이 급격하게 증가하고 있는 현실에서 이동·무선 환경에 대한 개인정보 침해, 모바일 악성코드 등 새로운 보안 위협의 확대가 예상되고 있다. 특히, 스마트 IoT 기기 등 경량형 IoT 장치에서 실행되는 웜, 바이러스는 IoT 기기 장치의 성능저하, 사용자의 개인 정보 불법 수집, 다른 서비스로의 바이러스 전파 등을 야기시킬 수 있어 이에 대한 대비가 무엇보다 중요하다. 또한, IoT 기기의 도난/분실, IoT 기기 내부에 저장된 정보의 유출에 대한 우려가 제기되고 있다. 뿐만 아니라, 개방형 IoT 플랫폼에 대한 시장 선호도가 높아짐에 따라 RIOT[3], Contiki[4] 와 같이 개방형 플랫폼이 사용된 IoT 기기가 주요 해킹의 표적이 될 가능성이 많아지고 있다. 이와 같이, IoT 기기에 대한 개방형 플랫폼을 중심으로 하는 서비스 확대와 함께 보안 위협의 증대는 안티바이러스 백신과 같은 기존 소프트웨어 기반 솔루션으로는 대응에 한계가 있으며, 백신 등과 같은 응용서비스 수준의 보안 대책으로는 사용자가 모르는 상태에서 IoT 기기가 루팅되어 내부의 중요한 정보가 유출되는 등의 위협에 대해서는 방지하기가 매우 어렵다. 특히, 국내 IoT 기기 보안 기술은 연구 초기 수준이라 엔드투엔드 통신보안 기능 등과 같은 응용 수준의 단품형 기술로 구성되어 있으며, 비교적 초기 단계의 기술이라고 할 수 있다.

IoT 기기의 저전력, 저용량, 멀티미디어 서비스, 실행 환경 등의 특성을 고려하여, 위에서 언급한 다양한 보안 위협으로부터 개방형 플랫폼 환경의 스마트 IoT 기기를 보호하기 위한 시스템 수준의 보안 플랫폼 기술 개발이 최우선적으로 요구되고 있다. 특히 기존의 서비스 도메인에 있는 사물들이 네트워킹이 되면서 IoT 기반의 다양한 신규 서비스가 증가하고 있으며, 이와 더불어 새로운 IoT 서비스의 활용도는 점점 높아지고 있다. 증가하는 신규 서비스는 삶의 편의성을 제공함과 동시에 다양한 보

안위협을 초래하고 있어, 보안 위협과 악의적인 공격에 대비할 수 있는 IoT 기기 보안 플랫폼의 개발이 필요하다.

본 고에서는 최근 들어 급증하는 사물인터넷에 의한 초연결 환경과 사물인터넷에 대하여 알아보고 초연결 환경에서 보안 위협에 대응하는 사물인터넷 보안 기술에 대한 연구와 표준화 동향을 알아보고 이를 위한 보안 기술의 방향을 알아본다.

Ⅱ. 사물인터넷 특성

본 장에서는 초연결 환경을 이루는 사물인터넷 서비스 인프라와 사물인터넷의 특성에 대하여 알아본다.

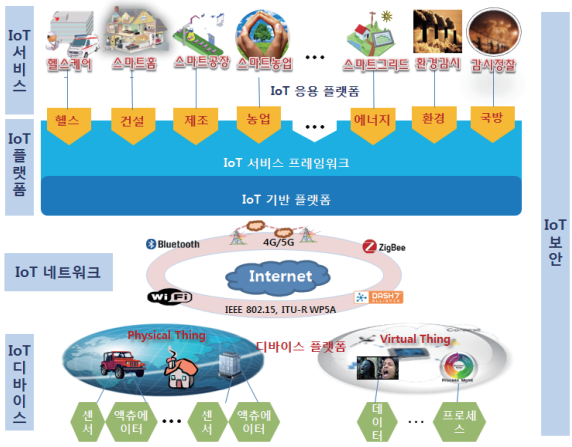

그림 2. 사물인터넷(IoT) 서비스 인프라

1. 사물인터넷(IoT) 서비스 인프라

〈그림 2〉는 사물인터넷 서비스 인프라를 나타낸 것으로 실 세계와 가상세계에 존재하는 사람, 사물, 프로세스, 데이터 등 모든 것 (Everything) 들이 인터넷으로 상호 연결되어 서로 소통하고 작용하는 지능형 서비스 인프라를 보여준다.

이를 통해서 이루어지는 사물인터넷 서비스는 물리/가상 사물을 연계하고, 협업하여 지능형 서비스를 제공하는 IoT 플랫폼, 모든 사물을 인터넷을 통해 상호 연결하여 소통하는 IoT 네트워크, 사물을 지능화시켜 스마트 인터렉션을 제공하는 IoT 디바이스, 프라이버시 보호와 안전한 시스템 운영을 보장하는 IoT 보안 등에 기능을 제공한다.

2. 사물인터넷(IoT) 특성

사물인터넷(IoT)이란 사람, 기기, 공간, 데이터 등 모든 것이 인터넷으로 연결되어 정보가 생성 · 수집 · 공유 · 활용되는 초연결 인터넷을 말한다. 특히 디바이스는 서비스 지향적이고 개방형이며, 각 디바이스들이 전력, 메모리, CPU, 생존 기간 등 다양한 성능 격차를 가지고 있고 대부분 오픈 소스에 IP가 내장되어 있는 특징을 가진다. 네트워크는 HW자원, 통신방식, 보안구조 등이 상이한 초연결 네트워크로 저전력의 통신망과 멀티홉 라우팅 통신을 하는 특징을 가진다. 서비스/플랫폼은 Open API 기반의 IoT 서비스를 제공하며 멀티 도메인 환경에서의 서비스 플랫폼 등을 가지는 특징을 가진다.

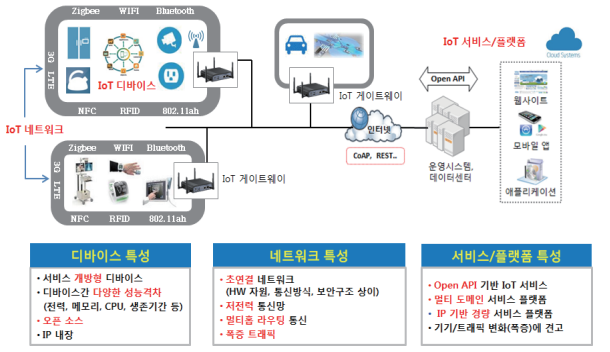

그림 3. 사물인터넷(IoT) 특성

- 서비스/플랫폼은 Open API 기반의 IoT 서비스를 제공하며 멀티 도메인 환경에서의 서비스 플랫폼 등을 가지는 특징을 가진다.
- 네트워크는 하드웨어 자원, 통신방식, 보안구조 등이 상이한 초연결 네트워크로 저전력의 통신망과 멀티홉 라우팅 통신을 하는 특징을 가진다.
- 특히 디바이스는 서비스 지향적인 개방형이며, 각 디바이스들이 전력, 메모리, CPU, 생존 기간 등 다양한 성능 격차를 가지고 있고 대부분 오픈 소스에 IP가 내장되어 있는 특징을 가진다.

Ⅲ. IoT 보안 위협

IoT 기기들의 스마트한 서비스를 위해 필수기능 이외에 추가 기능 모듈이 제공되고 있으나, 보안이 취약한 부분을 통한 기기 해킹이 가능해서, 개인과 사회의 안전에 치명적 영향을 미칠 수도 있다. IoT 기기의 대부분의 위협 사례는 기기의 취약 모듈을 통해 침입한 후, 중요 모듈로 접근하는 형태이므로 기기 운영 환경의 보안과 기기 내 각 기능별 위협의 확산 방지가 중요함을 알 수 있다. 스마트 홈, 스마트 헬스케어, 스마트 자동차 등 광

범위한 영역에서 빠르게 폭증하는 사물 인터넷은 정보 유출과 오작동의 진원지 또는 악성코드와 스팸을 퍼뜨리는 유포지가 될 수 있다. 해킹 사례를 보면 다음과 같다

그림 4. 사물인터넷(IoT) 기기 보안 위협 사례

IoT 보안 위협은 디바이스, 네트워크, 서비스/플랫폼 등 각 분야 별로 이루어진다. 디바이스의 경우에는 기기 정지나 오작동 유발에 의하여 인프라 마비 등과 같은 치명적인 위협이 일어날 수 있으며, 기기 분실/도난, 기기 위변조 등에 의해 개인정보 변조 또는 유출이 일어날 수 있다. 또한 디바이스 간에는 안성코드 전이 등에 의한 공격의 위협이 있을 수 있다. 두 번째는 네트워크의 경우에는 이기종 IoT 네트워크 간 연동 과정에서 정보 변조 또는 유출이 일어 날 수 있으며, 네트워크와 게이트웨이 등의 해킹 공격에 의한 라우팅 불통 등이 일어날 수 있으며 대단위 사물봇에 의한 IoT 서비스 거부 공격 등이 일어날 수 있다. 마지막으로 서비스/플랫폼의 경우에는 불법 포획 후 암호키 해킹에 따른 플랫폼 붕괴의 위협과 클라우드, 빅데이터 환경이므로 개인정보 유출이나 프라이버시의 위협이 일어난다. 이러한 다양한 디바이스 보안 위협으로부터 IoT 기기를 보호하기 위해 디바이스 플랫폼 수준의 보안 기술이 필요하다.

이러한 사물인터넷 환경에서의 보안위협을 막기 위한 보안 기술은 〈그림 5〉와 같이 크게 서비스 영역에 따라 IoT 서비스/플랫폼 보안, IoT 네트워크 보안, IoT 디바이스 보안으로 구성된다.

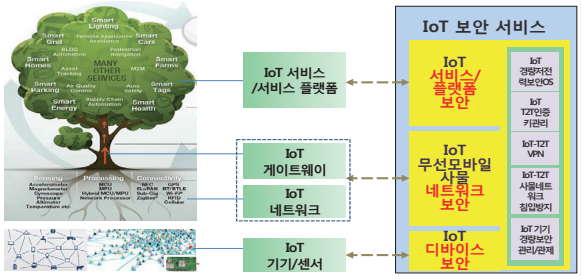

그림 5. 사물인터넷(IoT) 보안 구성도

이에 따라 기존의 정보보호 기술을 기반으로 사물인터넷에서 궁극적으로 추구하는 비전을 실현하고자 다양한 IoT 디바이스 환경에 적용되는 가볍고 신뢰할 수 있는 보안 서비스(인프라)를 제공하는 연구가 최근 전세계적으로 진행되고 있다.

Ⅳ. 국내외 연구 동향

본 장에서는 IoT 보안 관련한 국내외 연구 동향에 대하여 알아본다.

1. 국외 연구 동향

가. IoT 서비스/플랫폼 보안 – 암호

암호 관련한 연구로는 저전력/경량형의 암호, 해쉬, 키관리 기술 등의 연구가 선진 각국에서 이루어져왔다.

- (저전력 암호) Sheffield대학에서2010년에 100kHz 클럭에서 0.692uW급 소비전력 (9.23nA/kHz)으로 동작하는 저전력 AES 암호 설계/구현하였다.
- (경량 대칭키) 미국 NSA에서 2013년에 1~2천 게이트(GE) 이하로 경량 블록암호 알고리즘(SIMON, SPECK, KATAN, PRESENT, AES)을 구현하였다.
- (경량 공개키) 벨기에 루벤대학에서 2007년에 타원곡선 알고리즘을 500kHz 동작주파수에서 30uW급 전력, 14,000 GE 수준으로 구현하였다.
- (경량 해쉬함수) 터키 METU에서는 2010년 SHA-3 표준 알고리즘(Keccak-128)을 0.13um 공정에서 5,000 GE급 경량 해쉬 구현하였다.
- (키 해킹 방지) 독일 Bochum대학에서는 2006년에 1078 Byte ROM과 16 Byte RAM을 추가하여 부채널 공격에 의한 키 해킹 방지형 AES를 구현하였다.
- (키생성) 미국 MIT대학에서는 2007년에 0.48% 오류 수준의 PUF(물리적 복제방지) 기반의 비밀키 생성 기술을 확보하였다.

나. IoT 서비스/플랫폼 보안 – 인증/인가

인증/인가 관련한 연구로는 경량 사용자 인증 프로토콜, 기기간 인증 기술 등의 연구가 선진 각국에서 이루어져왔다.

- (경량 인증) LPN을 응용한 경량 사용자 인증 프로토콜인 HB(2001)를 개선한 HB-MP+(2008) 프로토콜은 2m bit(m: 바이너리벡터)의 통신 오버헤드와 보안성 개선하였다

* LPN(Learning Parity with Noise): 에러가 포함된 샘플에서 parity를 학습하기 어려운 문제임

– (T2T 인증)Syracus대학에서 2005년에 WSN을 위해 공개키 기반의 인증방식 경량화(ECDSA 대비 14%수준의 에너지 소모하는 연구를 하였다.

– (인증 프로토콜) 카네기멜론 대학에서 2002년에 WSN에서 BS의 브로드캐스트 메시지를 인증하기 위한 μTESLA 프로토콜을 개발하였다.

– (M2M인증) OneM2M(글로벌 개방형 M2M서비스 플랫폼) 표준화 단체에서는 M2M기기, 게이트웨이, 서버 네트워크 환경에서 인증, 암호 통신, 원격 신뢰 관리, 키관리 등 보안 관리 규격 개발 진행하였다.

다. IoT 서비스/플랫폼 보안 – 프라이버시

프라이버시 관련한 연구로는 프라이버시 정책 관리 기술 등의 연구가 선진 각국에서 이루어지고 있으나 아직은 연구 초기 단계이다.

– (프라이버시 정책 자율협상) 네덜란드 Twente 대학에서는 2008년에 개인정보를 프라이버시 협상 수준에 따라 추상화하여 다른 디바이스와 공유하는 QoC-Aware Privacy Policy 프레임워크 기술을 연구하였다.

라. IoT 네트워크 보안

네트워크 보안 관련한 연구로는 IPSO, OneM2M 등에서 IoT 기기제어 및 보안관리 표준규격이 개발 진행 중이며, 상용제품은 현재 자원제약 없는 무선·모바일 기기 중심으로 개발되고 있다.

– (초연결 보안) AllJoyn(퀄컴)에서는 IoT 연결성 플랫폼인 앱단위의 기본적인 인증, 암호 기능을 제공한다.

– (보안 게이트웨이) 인텔, 어드벤택, 유로텍, 프리스케일 등은 다수의 IoT 게이트웨이를 출시하고 있으나 상이한 하드웨어 자원· 통신방식·보안구조를 지원하는 초연결성 보안 기능은 지원하지 않는다.

– (암호/키관리) 키분배·암호·인증 기능이 포함된 다수의 Zigbee(Atmel, TI, EM 등), BLE(CSR, connectBlue, TI 등) 칩·솔루션 등은 있으나 IoT 환경을 고려한 키(대칭키, 경량 공개키) 관리 기술은 연구 진행 중이다.

– (이상행위 탐지) Michigan대에서 2005년에, Carnegie Mellon에서는 2010년에 WSN에서 센서 탑재코드 원격 검증을 통해 이상 센서 탐지기법에 대한 이론적 연구가 진행되었다.

– (폭증트래픽) 주니퍼, 버라이존, HP, Checkpoint, vArmour, Radware 등은 NFV/SDN/클라우드 기반 보안 솔루션 개발을 활발히 진행하고 있다.

– (종단보안) 스위스 취리히 대학에서는 2013년에 X.509 인증서(2,048bit-RSA키), TPM, DTLS 프로토콜을 이용하여 T-2-IoT 서버간 경량/저전력(18kB-RAM, 63kB-ROM/485,2mJ급) 상호인증 및 단대단 보안기술을 구현하였다.

마. IoT 디바이스 보안

디바이스 보안 관련한 연구로는 IoT 단말 제작 회사들이 제공한 오픈 하드웨어 형태의 통합 개발 환경을 이용한 다양한 D.I.Y 보안 디바이스가 개발되고 있다.

– (IoT 단말 제작 회사) Arduino, ioBridge iota, ARM mbed 등 D.I.Y IoT 디바이스 개발 업체와 Silicon Labs, NXP, Freescale, STM, TI 등 하드웨어 업체 들을 중심으로 IoT 단말 들이 제작 되고 있다.

– (하드웨어 보안) Silicon Labs의 EM358x 제품군은 32-bit ARM Cortex-M3 프로세서, 256~512KB-Flash, 32KB~64KB-RAM 사양을 갖춘 ZigBee 통신 SoC로 저전력(27mA(Rx), 31mA(Tx)) 사양을 지원하며, 메모리 보호 및 AES-128 암호 엔진 등 하드웨어 기반 보안 기능을 제공한다.

– (통신보안) Escrypt의 차량간 통신보안모듈 CycurV2X는 ECC 인증서 및 AES-CCM 암/복호화 지원하며 초당 400개의 메시지에 대한 서명 기능을 제공한다.

– (보안OS) IoT 디바이스용 RTOS(tinyOS, Contiki, RIOT 등)에서 링크 계층의 메시지 무결성 및 암호 기능을 제공한다.

– (기기보안) Gemalto사도 M2M 기기용 기기 인증 및 신뢰 통신 보안 서비스 제공 기술 연구·개발을 진행하고 있다.

2. 국내 연구 동향

가. IoT 서비스/플랫폼 보안 – 암호

국내에서는 저전력/경량형의 암호, 해쉬, 키관리 기술 등의 연구가 이루어져 왔다.

– (저전력) ETRI에서는 2012년에278kHz 클럭에서 3.5uW급 소비전력(10.49nA/kHz) 으로 동작하는 수동형 RFID용 AES 암호 설계/구현하였다.

– (경량 대칭키) 수동형 RFID 적용가능 수준의 3,100 GE급 대칭키 블록암호(HIGHT) 설계/구현 기술 및 표준을 확보하였다.

* 국내 경량 대칭키 블록암호 표준: HIGHT(TTA, 2006),

LEA(TTA, 2013) 등이 있다.

– (경량 공개키/경량 해쉬) 경량 공개키 및 해쉬 기술에 대한 연구는 아직은 연구 초기상태이다.

– (키해킹 방지) ETRI에서는 2011년에 보안 HW칩의 국내 암호(ARIA) 키 크랙킹 방지 및 경량 (1KB"RAM & ROM") 부채널 분석 방지 기술을 개발하였다.

* LG CNS에서는 2010년에 부채널 공격에 의한 IC카드 SEED 암호키 해킹을 방지하는 전자여권을 개발하였다.

나. IoT 서비스/플랫폼 보안 – 인증/인가

인증/인가 관련된 기술은 국내에서 저전력/경량화, T2T 등의 인증 기술 등의 연구가 이루어져왔다.

– (저전력/경량화) 덕성여대에서는 2012년에 HMAC이 지원되지 않은 저전력 경량 기기(Arduino: 32KB 메모리, 2KB SRAM) 에서 256bit AES키를 사용하여 MD5 해시기반 574ms 급 DTLS 상호인증을 구현하였다.

– (T2T 인증) 연세대에서는 2013년에 HB-Family 프로토콜에서 동기화 문제를 해결하고, 통신비용을 k(응답 메시지의 비트 수)+1로 개선하였다.

* HB-family 프로토콜: 일정 확률로 틀린 인증 응답을 생성하여 공격자가 비밀키를 유추하기 어렵게 만드는 경량 인증 프로토콜이다.

* CCTV, 셋탑 등 HW자원 및 전력 제약이 없는 IoT 기기인증용 PKI기술 및 국내외 표준을 확보하였다.

– (상황인지) 스마트폰 센서를 이용하여 사용자의 상황을 인지하고, OWL 모델을 사용하여 사용자의 특성을 고려한 스마트 홈 제어 기술을 보유하였다. (경희대, 2010)

다. IoT 서비스/플랫폼 보안 – 프라이버시

프라이버시 관련 분야 에서도 프라이버시 보호를 위한 프로토콜, 정책 등의 연구가 이루어져왔다.

– (프라이버시) ETRI에서는 2013년에 영지식 증명을 통한 프라이버시 보호형 전자서명기술 개발 및 ISO 국제표준 채택하였다.

* 영지식증명(Zero-Knowledge Proof): 이용자의 신분노출 없이도 자격의 정당성을 증명하는 암호 프리미티브이다.

– (RFID 프라이버시) ETRI에서는 2011년도에 모바일 RFID 서비스 사용자의 프라이버시 보호를 위한 프로토콜 정의 및 ISO/IEC 표준을 제정하였다.

– (프라이버시 정책 자율협상) 부경대에서 2010년에 프라이버시를 고려한 유비쿼터스 전자상거래에서 P3P에 기반한 협상 메커니즘인 P4P(Pervasive P3P) 기술을 개발하였다.

라. IoT 네트워크 보안

초연결 보안, 보안관리, 침입감시 등의 연구가 이루어져왔다

– (초연결보안) KETI와 SKT 공동으로 2014년도에는 IoT 연결성 지원(MOBIUS) 및 IoT 게이트웨이 플랫폼(&CUBE) 기술을 보유하고 있으며, 보안은 SSL 기반 암호화·인증만을 지원하는 수준의 기술개발을 진행하였다.

* 암호/인증이 포함된 상용 ZIGBEE 센서 용 프로토콜 기술을 보유(레이디오펄스, KETI 등)하고 있으나 공유키 방식으로 IoT 환경을 고려한 키(대칭키, 경량 공개키) 관리 기술은 개발되지 않았다.

– (보안관리) OneM2M의 기기관리 프로토콜 개발(SKT, KETI)을 진행하고 있으나, 기기 신뢰성 관리 등 보안관리 기술은 아직 개발되지 않았다.

* 현재 상용 제품은 자원제약 없는 무선·모바일 기기 보안관리 중심이다.

– (침입감시) 경량·저전력 기기 및 다양한 무선 통신이 존재하는 T2T 환경에서의 침입 감시 기술은 현재 기초 연구 수준이다.

* 인하대에서는 2007년에 WSN에서 센서에 탑재된 코드의 무결성을 원격에서 검증하는 이론적인 연구를 일부 진행 하였다.

* ETRI, 삼성전자, 코닉글로리, 유넷시스템 등은 WLAN 프로토콜(802.11b/g/n/ai) 및 WLAN 칩을 탑재한 단말 (AP, 노트북, 스마트폰 등)을 대상으로 하는 무선침입·해킹탐지 기술을 보유하고 있다.

– (폭증트래픽) KAIST, 성균관대 등은 NFV/SDN 보안 취약성 분석 등 실험실 수준의 초기연구 단계이다.

* SDN 콘트롤러(아토리서치, 나임네트웍스, ETRI), SDN 스위치(파이오 링크), NFV 기반 LTE코어장비 (SKT/삼성전자) 등 SDN/NFV 구축을 위한 요소기술은 일부 확보하고 있다.

– (종단보안) 경량·저전력이 고려되지 않은 기능검증 수준의 서버·RFID 리더간 DTLS 기반 보안 기술 구현 사례(ETRI)가 있으며, 자원제약이 없는 디바이스에 대한 VPN 기술을 확보하고 있다.

* 펜타시큐리티에서는2014년에PKI 및 IEEE1609.2기반 차량 통신 보안 기술 구현– 초당 32.4개의 인증서 발급하는 기술을 개발하였다.

마. IoT 디바이스 보안

디바이스 보안 관련하여서는 하드웨어 보안, 보안OS, 기기보안 등의 연구가 이루어져 왔다.

– (하드웨어 보안) ETRI에서는 2014년에 스마트폰 급 디바이스 환경에서 HW 기반 신뢰 보안 기능을 제공하는 초소형 MTM 보안 기술을 개발하였다.

* (스펙) ARM cortex-M3 MCU, 35KB-RAM, 1MB-Flash, 동작주파수 24MHz, 소모전류 10mA급 (주요기능) Secure booting, MTM 기반 무결성 검증 및 키 관리 모듈 등

– (보안OS) ETRI에서는 경량 IoT 센서(8bit, 16bit 저전력 MCU급)용 초소형 (〉50KB급), 초절전(〈20mA급) 운영체제 NanoQplus 개발하였다.

* NanoQplus 보안기능: 6LoWPAN을 위한 무선 링크 보안(AES-128, ARIA 암호)만을 제공한다.

– (기기보안) KETI에서는 경량 IP프로토콜 (CoAP, MQTT, 6LOWPAN 등)을 내장한 개방형 IoT 디바이스 플랫폼을 개발하였고 ETRI에서는 스마트 IoT 미들웨어 플랫폼을 개발하였으며, 아직 해킹 방지 등의 보안 기능은 제공하지 않는다.

V. 표준화 동향

본 장에서는 IoT 보안 관련한 표준화 동향에 대하여 살펴본다.

사물인터넷 관련 기술들의 표준화는 ITU(International Telecommunication Union)와 유럽의 ETSI(European Telecommunications Standards Institute)가 서비스 모델과 서비스 연동의 관점에서 구조적으로 접근하고 있으며, IETF에서 IP 기반 프로토콜 표준을 주도하고 있다. 이외에도 IPSO(Internet Protocol of Smart Objects), OMA(Open Mobile Alliance) 등의 사설 표준 기관에서도 IoT 관련 표준 적용을 논의하고 있는 중이다.

사물인터넷 보안 기술은 아직 표준화 초기 단계로 차후에 이루어질 본격적인 표준화를 위한 사전 작업들이 이루어지고 있으며, 대표적인 기관으로 Internet Engineering Task Force (IETF)가 장기적 관점의 사물인터넷 기술 표준화를 담당하고 있다.

현재 IETF에서는 다양한 무선 접속 네트워크 환경에 IP를 적용할 수 있는 기술들을 표준화하기 위해 6LowPAN, 6Lo, 6tisch, ROLL, LWIG 등의 워킹 그룹(WG: Working Group)들을 결성하였으며, 또한 IETF에서는 사물인터넷을 구성하는 소형 장치 간 전송되는 데이터의 암호화와 무결성 제공을 위해 DTLS의 재사용을 권고하고 있고, 정보 자원의 사용 인가와 제어를 위한 다양한 기술들에 대한 논의가 진행되고 있다.

VI. 결 론

본 고에서는 IoT 보안 위협 사례와 더불어 연구 및 표준화 현황을 살펴보고 각 서비스/플랫폼, 네트워크, 디바이스 분야별로 앞으로의 연구 방향에 대하여 알아본다.

1. 서비스/플랫폼 보안 – 암호

암호 관련하여서는 키해킹에 안전한 저전력·경량·고속 암호 알고리즘 및 기존 암호 알고리즘 저전력·경량 구현 기술 필요하다

- 특히 MHz 단위의 IoT 디바이스에서 전력소모를 줄이기 위해서는 kHz 클럭 수준과 수천 GE급의 경량/저전력 암호모듈 연구가 필요하다.
- 대칭키 암호의 경량·저전력 기술의 국제경쟁력을 확보하고 있어, 이를 기반으로 상대적으로 열세인 공개키 암호 및 해쉬의 경량·저전력 설계 기술격차 축소를 위한 집중적인 개발이 필요하다.

2. 서비스/플랫폼 보안 – 인증/인가, 프라이버시

클라우드·빅데이터 기반 IoT 서비스 환경에서 보안연동 및 프라이버시 보호를 위한 크로스도메인 IoT 경량 보안 서비스 플랫폼 기술 확보가 필요하다.

- 국외에 비해 저사양 디바이스에 대한 인증/인가 기술에 열세를 보여 이에 대한 집중적인 기술개발이 필요하다.
- IoT환경에 특화된 프라이버시 보호 기술 연구는 국내외 초기 단계이므로, 원천기술 확보를 통한 기술 선점이 필요하다.

3. IoT 네트워크 보안

보안이 취약한 경량 디바이스로 구성된 사물네트워크에 트러스트 보안 中心 센터 기능을 제공하는 경량 IoT 보안 게이트웨이 및 초연결 기기에 대한 무인원격 보안관리 서버 新기술 개발이 필요하다.

- 국내외 초기연구단계로 기술격차가 크지 않고, IoT 신뢰 네트워크 구축을 위한 핵심원천기술로 기술선점을 위한 경쟁이 치열할 것으로 예상된다.

4. IoT 디바이스 보안

HW 제약·성능 등이 상이한 이기종 디바이스를 위한 기기 맞춤형 보안 운영체제와 경량/저전력 디바이스 성능, 응용에 특화

된 보안 HW 모듈 등 IoT 디바이스의 高가용성 보장을 위한 보안 기술 개발이 필요하다.

- 저전력/경량 IoT 디바이스용 RTOS 안전성을 위한 보안 기술은 국내외 기술 격차가 크지 않아 차별화된 보안 기술 선점이 필요하다.
- 저가/저전력 IoT 기기에 적합한 HW 기반 보안 기술은 국내외 기술 격차가 다소 있어 기술 선점을 위한 차별화 전략이 필요하다.

Acknowledgement

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (B0190-16-2032, Development of Operating System Security Core Technology for the Smart Lightweight IoT Devices)

참고문헌

[1] Davies R. W." The Data Encryption standard in perspective, "Computer Security and the Data Encryption Standard, pp. 129-132. (http://www.nist.gov/aes).

[1] D.Y.Kim, S.H.Kim, at el., "Internet of Things Technology and Development Direction", KICS, Journal of Information and Communication, Vol. 28, No.9, pp.49-57. Sept 2011

[2] C.S.Pyo, H.Y.Kang. at el., "IoT(M2M) Technology Trends and Development Prospects", KICS, Journal of Information and Communication, Vol. 30, No.8, pp.3-10. Sept 2013

[3] Baccelli, Emmanuel, et al. "RIOT OS: Towards an OS for the Internet of Things." Computer Communications Workshops (INFOCOM WKSHPS), 2013 IEEE Conference on. IEEE, 2013

[4] Dunkels, Adam, Bjorn Gronvall, and Thiemo Voigt. "Contiki-a lightweight and flexible operating system for tiny networked sensors." Local Computer Networks, 2004. 29th Annual IEEE International Conference on. IEEE, 2004.

[5] H.Y KIM, H.U Park, G.A Shin, S.T Kim. "NanoQplus: Light-weight operating System for Internet of Things", KICS Conference, June 2015.

[6] IoT Markets, ABI Research, April 2014

[7] Mango Board, E-ToI NanoQplus Reference Board, http://www.mangoboard.com/sub2.html?catcode=121200&ii=3

[8] Kim Y.-H, Lee Y.-G, Kim J.-N, "TeeMo: A Generic Trusted Execution Framework for Mobile Devices," International Conference on Computer, Networks, Systems, and Industrial Applications (CNSI), pp.579-583, July 2012

[9] Kim Y.-H, Kim J.-N. "Building Secure Execution Environment for Mobile Platform," First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering, pp.119-122, 2011

약 력

김 정 녀

1987년 전남대학교 전산통계학과 학사
2004년 충남대학교 컴퓨터공학과 석사, 박사
1988년~현재 한국전자통신연구원 시스템보안그룹 PL(Project Leader)/책임연구원
1996년 OSF/RI 공동연구 연구원 (미국)
2005년 Univ. of California, Irvine Post-Doc.
2015년~현재 과학기술연합대학원대학교(UST), 정보보호공학과 교수
관심분야: IoT보안, 모바일 보안, 시스템 · 네트워크 보안, 보안 OS 등

진 승 헌

1995년 숭실대학교 전자계산학과 학사, 석사
2004년 충남대학교 컴퓨터과학과 박사
1994년~1996년 대우통신
1996년~1999년 삼성전자
1999년~현재 한국전자통신연구원 정보보호연구본부 본부장/책임연구원
관심분야: 컴퓨터/네트워크 보안, PKI, ID관리, 개인정보보호, 핀테크 보안