특집 06

사물인터넷상에서의 보안과 프라이버시 보호 이슈

서화정 · 이동건 · 김지현 · 최종석 · 김호원 (부산대학교)

목 차 »

1. 개 요

최근 국내외 학계와 산업체, 연구소에서는 사물인터넷(Internet of Things: IoT)에 대한 관심이 고조되고 있으며, 제2의 닷컴버블로 불릴 정도로 이에 대한 기술 및 서비스 개발, 투자가 진행되고 있다. 사물인터넷 기술은 기존의 유비쿼터스 기술이나 USN(Ubiquitous Sensor Network) 기술에서 지향하던 서비스를 고려해볼 때, 전혀 새로운 기술이라고 볼 수 없다. 하지만, 최근의 정보통신 환경의 급속한 변화, 특히, 웹 서비스 기술의 발전과 소프트웨어 플랫폼 기술, 클라우드 기술, 유/무선 통신 기술, 디바이스 경량화 기술, 센서 기술, 스마트 폰, 임베디드시스템 기술의 급속한 발전으로 인해 사물인터넷이라는 이름으로 시장에서 재조명 받고 있는 것이다. 기존 국내에서 많은 연구/개발, 투자가 있었던 USN 분야는 기술 개발 중심으로 진행했었기 때문에 시장에서 그다지 성공적이지 못했다고 볼 수 있다. 반면, 사물인터넷은 특정 기술 중심이 아니라 서비스 와 사용자 관점, 시장 관점에서 사물인터넷을 보고 있기 때문에 시장에서의 성공 가능성이 매우 높다고 할 수 있다. 아래 (그림 1)은 USN 산업발전 전략 보고서[1]에 기술되어 있는 사물인터넷 기술 개념도이다. 그림에서 사물인터넷 기술은 IoT 혹은 WoO(Web of Object)로 언급되어 있다. 사물인터넷은 사물(Thing)과 사람(Human), 미디어/서비스의 3대 요소로 구성되며 사물인터넷을 실현하는데 필요한 제반 기술로는 웨어러블 기술, 스마트 홈 기술, ICT 모듈 기술, 스마트컴퓨팅 기술, 스마트미디어 기술, 스마트

(그림 1) 사물인터넷 기술 개념도

플랫폼 기술이 언급되어 있다. 또한, 사물인터넷 분야의 응용 서비스 시장으로 전통산업 분야, 생활 밀착형 분야, 사회 안전 분야, 신산업 분야가 제시되어 있다.

이처럼, 사물인터넷 기술은 특정 기술 중심이 아니라, 여러 기술의 복합체이며 시장 중심적 관점에서 해석되고 있음을 알 수 있다. (그림 2)는 사물인터넷 서비스 실현 기술을 보여주고 있다. 사물인터넷 서비스는 데이터를 센싱하고 센싱한 데이터를 처리하여 정보를 얻으며, 이를 토대로 의미있는 지식을 얻고 이를 활용하는 기본 구조를 가진다.

이 때문에 데이터 센싱 단계에서는 온도, 습도, 움직임, 소리 등 환경 정보를 센싱하는 기술과 사람의 행동 패턴 등을 센싱하는 기술이 필요하다. 즉, 사물인터넷 분야에서의 센싱은 물리 정보 센싱뿐만 아니라, 사람이나 서비스 프로파일, 행동 양식, 동작 특성 등의 정보를 처리하여 데이터를 얻는 것도 센싱 영역에 속한다. 또한, (그림 2)에 언급 되어 있는 것처럼 이러한 센싱 분야는 개념적으로 다중 인식(Perception) 개념으로까지 영역을 확대 해석될 수 있다. 또한 센싱된 데이터는 기본적으로 빅데이터로 볼 수 있으며, 해당 센싱 빅데이터에 대한 다양한 데이터 마이닝 기법과 머신 러닝 기법, 상황 인지 기법을 통해 의미 있는 정보를 얻을 수 있다. 그림에서 언급된 지식 마이닝도 이에 포함된다. 사물인터넷의 주요 디바이스는 임베디드 시스템으로

(그림 2) 사물인터넷 서비스 실현 요소 기술

볼 수 있으며, 사람과 서비스의 편의성을 좋도록 하기 위해 웹 서비스 연동 기술, 기존 SNS 연동 기술, 자연어 처리 기술 등이 필수적이라고 볼 수 있다.

하지만, 다양한 기술을 융복합적으로 사용하여 시장 친화적으로 접근하는 사물인터넷은 시장에서 성공하기 위해서는 법적인 규제와 보안/프라이버시 침해 문제를 우선적으로 해결할 필요가 있다. 규제는 각 국가별로 다양하게 존재하기 때문에(예: 한국에서의 원격 진료 이슈) 본 고에서는 논외로 하고 보안/프라이버시 침해 문제만을 살펴보기로 한다. 사물인터넷 기술의 내재적 다기술 융복합화 특성은 정보를 센싱하는 단계에서의 프라이버시 침해 문제를 야기할 수 있으며, 또한, IoT 디바이스와 서비스에서 보안 취약성/프라이버시 침해 문제, IoT 디바이스간 통신/네트워킹에서 보안 문제, 센싱 데이터 보관 및 처리 단계에서 보안/프라이버시 침해 문제 등 다양한 보안/프라이버시 침해 문제를 야기할 수 있다.

이에, 본 고에서는 2장에서 사물인터넷 보안/프라이버시 보호 기술에 대해 사물인터넷 디바이스 레벨과 디바이스간 통신/네트워크 레벨, 데이터 수집/보관/처리 단계, 서비스 레벨에서 살펴보고자 한다.

2. 사물인터넷 보안 기술

사물인터넷은 전술한 것처럼 다양한 기술을 융복합적으로 사용하여 사용자에게 편리하고 다양한 서비스를 제공한다. 이 때문에 보안 취약성 및 프라이버시 침해 문제가 사물인터넷을 구성하는 각 요소 기술마다 존재할 수 있으며, 또한 요소 기술간 연결 인터페이스 부분에서도 존재할 수 있다. 그리고 기술간 연동시 예상치 않은

새로운 보안 취약성도 나타날 수 있다. 이 때문에 안전하고 신뢰할 수 있는 사물인터넷 서비스를 제공하기 위해서는 우선 사물인터넷 서비스 구성 기술 요소 각각에 대한 보안 기술을 체계적으로 살펴볼 필요가 있다. 먼저, 센싱 기능과 센싱된 데이터에 대한 통신, 네트워킹 기능, 사용자 인터페이스 제공 등, 사물인터넷 서비스에서 핵심 역할을 수행하는 디바이스에서의 보안 이슈를 살펴본다.

2.1 사물인터넷 디바이스 보안 이슈

2.1.1 디바이스 인증/식별 기술

사물 인터넷에서의 디바이스 인증 및 식별은 매우 중요한 기술이다. 예를 들어, 권한이 없는 제 3자가 악의적으로 설치하여 거짓 정보를 제공하는 센싱 디바이스로 인해 임의로 난방을 켜고 끄는 등의 피해를 방지하기 위해서 디바이스에 대한 인증 및 식별은 반드시 필요한 절차라고 할 수 있다. 하지만 사물인터넷을 구성하는 장치에 대한 인증 및 식별 기능을 구현하는 것은 쉬운 일이 아니다. 그 첫 번째 이유는 사물인터넷에 연결되는 디바이스의 개수가 수십억 개에 달할 것으로 예측되기 때문이며, 또 다른 이유는 사물인터넷을 구성하는 장치들 중 대부분의 장치는 연산 능력이 떨어지거나 메모리가 적을 가능성이 높고, 배터리를 탑재해야 하는 등 제한적인 연산 능력을 갖추게 될 것이라는 것에 있다. 사물인터넷은 가정 및 산업뿐만 아니라, 점차 사회 공공 분야에 까지 확대될 조짐을 보이고 있으며, 이러할 경우 사물인터넷이 공격을 받게 되면 기존의 PC나 스마트폰에서의 해킹과는 차원이 다른 막대한 손실을 발생시킬 수 있다.

사물인터넷에서 주로 사용될 것으로 예상되는 인증 및 식별 기술로는 인증서를 이용한 방법, ID/패스워드를 이용한 방법, 그리고 SIM (Subscriber Identity Module)을 이용한 방법 등이 있다. 인증서를 이용한 방법의 경우 이미 많은 분야에서의 경험을 통해 안정적이고, 강력한 인증을 제공하는 장점이 있지만, 연산량이 많아서 자원 제약적인 디바이스에는 한계가 있으며, CA(Certification Authority)를 필요로 하는 등의 단점이 있다. ID/패스워드를 이용한 방법은 이에 반에 매우 간단하며, 가볍다는 장점이 있지만, 대량의 디바이스에 적용하기에 한계가 있다. SIM의 경우 플라스틱 카드 형태가 주류이지만, 회로 기판에 바로 부착되어 사물인터넷 디바이스에 사용될 수 있는 형태인 Embedded-SIM이 제안되기도 하였다.

2.1.2 디바이스 접근 제어 기술

사물인터넷에서는 전통적인 접근 제어 방식들이 가지던 이슈들을 비롯하여 분산되어 있는 많은 디바이스들을 커버 할 수 있을 만큼 확장이 용이한지, 또한 유동적인 사물인터넷 환경을 얼마나 잘 반영할 수 있는지, 그리고, 자원 제약적인 디바이스에 적용 가능한지가 중요한 이슈가 된다. 역할을 기반으로 접근 제어를 수행하는 RBAC(Role Based Access Control)[2,3]의 경우 제어 규칙을 관리하기 위한 비용은 적지만, 규칙의 폭발적인 증가를 수용하기 어려운 단점이 있으며, 속성 기반의 ABAC(Attribute Based Access Control)[4]은 사용자의 속성을 바로 사용함으로써 규칙을 잘 다룰 수 있지만, 도메인 안팎의 속성들을 동일하게 일치시켜야 하는 어려움이 있다. 또한 두 방법 모두 최소한의 권한만을 체크해 리소스를 허가하지 않으며, 모든 권한을 살핀 후에야 허가를 줄 수 있는 단점이 있으며, 권한을 위임하는 것이 어려운 등 유동적이지 못하다.

이러한 문제는 디바이스의 수가 증가할수록 더 심각해지는데, 사물인터넷 환경에는 CapBAC (Capability Based Access Control)[5,6]이 주목을 받고 있다. 이는 특정 리소스를 사용할 수 있는 권한을 요청시 Token을 발급하여 사용할 수 있게 하는 개념으로써, 권한 위임, 자격 철회 등이 지원이 되며, 자격을 매우 자세하게 기술할 수 있는 것이 장점이다. EU의 FP7 IoT@Work 프로젝트에서도 CapBAC를 확장한 형태의 접근 제어 기법을 제시하고 있으며[7], 타원 곡선 암호를 이용한 CapBAC에 관한 연구와[8], CapBAC에 대한 보안성 분석 등에 관한 연구가 진행된 바 있다[9].

2.1.3 디바이스 OS 보안 기술

사물인터넷의 디바이스들은 다양한 보안 위협에 노출되어 있으며, 언제든지 사이버 공격의 대상이 될 수 있는 가능성을 가지고 있다. 따라서 사물인터넷을 구성할 때는 보안에 대한 철저한 계획을 가지고 시작해야 한다. 보안 OS는 그 시작 단계로써, 운영체제 차원에서 자원에 대한 통제와 커널에 대한 보호, 시스템에서 일어나는 동작에 대한 감사 등의 기능을 수행하며, 기존의 PC 환경에서는 전통적인 운영체제들을 기반으로 보안 OS에 대한 연구가 진행되어 왔다. 특히 SELinux[10]의 경우 커널 단계에서 보호 기능을 수행하며, 자원에 대한 접근 통제 기능을 수행하며, 공격자에 의해 커널이 수정되는 것을 방지하기 위해 커널 보호를 수행한다. 또한, 침입에 대한 피해를 최소화하기 위해 프로세스 실행시 최소 권한만을 할당하며, 시스템에서 일어나는 보안 규칙에 어긋나는 일들을 파일로 기록하여 감사 자료로 활용할 수 있도록 하고 있다. 최근에는 사물인터넷을 구성하는 디바이스를 위한 임베디드 OS에도 보안 OS가 적용되려는 시도가 있는데, WindRiver사에서는 실시간 OS인 VxWorks에 보안 기능을 탑재 하였다[11]. 이 기능에는 모듈화를 통해서 시스템 코어와 관계없이 업그레이드 가능한 구조를 포함하고 있으며, 데이터 암호화, tamper proof, 보안 업그레이드, 신뢰할 수 있는 루트, 사용자 및 정책 관리 등의 보안 기능들을 제공한다.

2.1.4 디바이스 경량 암호/보안 프로토콜 기술

사물인터넷을 구성하는 디바이스 간의 통신에서의 보안을 위해 기밀성, 무결성에 대한 부분을 고려해야 한다. 이를 위해서는 암/복호화 및 해쉬 생성을 위한 프리미티브 및 이를 구현하기 위한 방안을 고려해야 한다. 사물인터넷을 구성하는 많은 장치의 경우 자원제약적인 경우가 많기 때문에, PC에서 주로 사용하던 전통적인 암호 방식을 그대로 적용하기에는 한계가 있다. 이들 프리미티브를 최적화 하기 위한 연구는 매우 오래 전부터 활발히 연구되고 있으며, 뿐만 아니라 새로운 경량 프리미티브에 대한 연구도 활발히 진행되고 있다.

암/복호화 알고리즘에 대한 대표적인 경량화 사례는 PRESENT[12], KATAN 및 KTANTAN[13], HummingBird[14] 등의 사례가 있으며, 국내에서도 HIGHT[15]와 LEA[16]와 같은 경량 암호화 알고리즘을 개발한 사례가 있다. PRESENT[12]는 4비트의 단순한 Sbox를 이용하며, 키 XOR 연산과 permutation 연산만을 이용하여, 암호화에 필요한 연산 비용을 최소화 하였다. KATAN 및 KTANTAN[13]은 2개의 LFSR을 기반으로 암호화를 수행하며, HummingBird[14]는 Rotor Machine을 모티브로 하여 RFID 등의 암호화를 위해 만들어진 경량 암호이다. HIGHT[15]는 32비트 단위

의 연산과 다중 Feistel 구조를 활용하며, LEA[16]의 경우 Add, Rotate, XOR(ARX)의 단순 연산만으로 암호화를 수행한다. 해쉬 함수 분야에서는 QUARK[17], Photon[18], SPONGENT[19]와 같은 경량 해쉬 함수가 개발되기도 하였다. QUARK[17]은 KATAN[13]과 Grain[20]이라는 경량 암호를 응용하여 만들어 졌으며, Photon[18]은 AES[21]와 유사하지만 가벼운 형태의 연산 구조를 가지며, SPONGENT[19]는 PRESENT[12]의 구조를 응용하여 만들어 졌다.

사물인터넷을 위한 무선 통신 기술로는 Wi-Fi[22], ZigBee[23], Bluetooth[24] 등이 예상되며, 각각의 통신 방법에서는 프로토콜의 보안을 위한 방법들을 제시하고 있다. Wi-Fi에서는 기밀성 및 무결성을 위해 사전 설정한 키를 바탕으로 통신 트래픽을 암호화 하며, MAC(Message Authenticatino Code)을 통해 무결성을 제공해주는 WPA(Wi-Fi Protected Access)기술을 제공한다. 이 기술에서는 AES-CCMP (AES-Counter Cipermode with Block Chaining Message Authentication Code Protocol)을 이용하는데, AES의 카운터 모드와 CBC 모드를 이용해 암호화를 수행하고, 무결성 체크 코드를 생성하여 기밀성 및 무결성을 제공한다. ZigBee는 IEEE 802.15.4의 PHY 및 MAC 계층을 활용하고 있으며, AES-CCM을 확장한 AES-CCM*를 사용하여 기밀성 및 무결성을 제공한다. Bluetooth는 데이터 전송률에 따라 BR(Basic Rate), EDR (Enhanced Data Rate), HS(High Speed), 및 LE (Low Energy)로 나누어 지는데, BR/EDR의 경우 암호화를 위해 LFSR 기반의 스트림 암호 암고리즘인 E_0이 쓰이며, 인증 과정에서는 SAFER+ 암호 기반의 E_1 알고리즘이 사용되고, LE의 경우 암호화를 위해 AES-CCM을 사용한다.

2.2 디바이스 통신 구간에서의 보안 이슈

2.2.1 CoAP, LwM2M 보안 기술

사물인터넷 서비스에서 사용되는 디바이스는 일반적으로 높은 자원 제약성을 가진다. 이 때문에 CoAP(Constrained Application Protocl)이나 LwM2M(Lightwegith M2M) 프로토콜이 개발되었다. CoAP은 인터넷을 통해 매우 제한적인 자원을 가지는 장비간 상호 통신이 가능하며 저전력으로 동작해야하는 센서와 스위치 디바이스 응용을 목적으로 만들어졌다[25]. CoAP은 application layer 프로토콜로써 HTTP로 쉽게 변환이 되어 웹에 통합 된다. 현재까지 CoAP 보안을 위한 표준은 DTLS(Datagram Transport Layer Security)이 있지만, 디바이스에서 구동하기 위해서는 CoAP 자체 보안을 개선해야할 필요가 있다 [26].

CoAP에 기반을 둔 LwM2M의 경우에도 oneM2M 파트너 쉽 프로젝트를 통해 활발히 진행되고 있다. LwM2M에서는 클라이언트와 서버간의 상호 인증을 기반으로 서비스가 제공된다. 기밀성과 무결성을 제공하기 위해 데이터는 암호화되어 상호간에 교환되어야 한다. CoAP 프로토콜의 UDP 채널 보안은 DTLS에 의해 정의되며 이는 HTTP 상에서의 TLS v1.2와 동일하다. LwM2M 프로토콜은 DTLS를 통해 인증 및 데이터 무결성과 기밀성을 제공함으로 가능한 오랜 기간 동안 DTLS 세션을 유지하도록 권고하고 있다. LwM2M 서버 상에서는 DTLS를 제공하기 위해 총 4개의 키관리 메커니즘을 정의하고 있다. 먼저 사전 키 분배를 통해 암호화를 수행하는 Pre-Shared Keys 모드는 AES_128_CCM_8 혹은 AES_128_CBC_SHA256를 통해 보안이 제공된다. Raw Public Key Certificate 모드의 경우에는 ECDH와 ECDSA를 이용하여 키

를 안전하게 교환하며 이를 통해 생성된 키는 이전과 같은 암호화 기법으로 암호화된다. X.509 서명을 사용하는 모드에서는 이전 모드에서 제공하는 암호화 기법을 적용하여 생성된 정보가 상호간에 교환되게 된다. 마지막으로 관리되는 게이트웨이 환경 상에서와 같이 보안이 필요치 않은 환경에서는 No Sec모드가 사용될 수 있다. 접근 제어 매커니즘은 접근제어 오브젝트 관리 프로세서에 의해 해당 권리를 요청하고 생성한 이후에 해당 오브젝트에 대한 접근 권한을 부여받는 방식으로 제공되고 있다.

2.2.2 MQTT 보안 기술

MQTT 프로토콜은 이기종의 기기간의 어플리케이션 메시지 통신을 지원하기 위해 만들어졌다. 이러한 디바이스는 매우 간단한 기기부터 복잡한 기기까지 포함할 뿐 아니라 어떠한 운영체제 및 소프트웨어를 포괄한다. 일반적으로 이러한 기기들은 인터넷과 같이 보안이 취약한 환경에서 동작되게 된다[27]. 따라서 MQTT 상에서의 End to End 통신 보안은 안전한 메시지 교환을 위해 선결되어야 하는 문제다. MQTT 프로토콜은 전송 계층 프로토콜이므로 메시지 전송에 관해서만 기술된다. 구현시 유저와 디바이스에 대한 인증 메커니즘이 필요하며 서버 자원에 대한 접근제어 또한 필요하다. 이와 더불어 어플리케이션 메시지의 무결성과 프라이버시 보호는 메타데이터를 포함하여 프로토콜 전반에 걸쳐 해결되어야 한다. 소프트웨어와 시스템은 악의적인 공격에 노출된다고 가정되며 이를 디자인하기 위해서는 많은 고려가 필요하다. MQTT 보안 레벨은 크게 Unsecured, Base Secured로 나뉜다. 먼저 Unsecured 레벨에서는 layering 과 tunnelling이 사용되지 않는 보안 레벨로써 SSH, IPsec/VPN 과 같은 프로토콜을 이용하여 보안을 제공한다. Base secured 보안 레벨의 경우 TLS 1.2에 의해 layer가 정의된다. 다른 프로토콜과의 연동을 위해 TLS는 정해진 파라미터를 사용하여 구현 되어야 한다.

2.3 데이터 수집/보관 단계에서의 보안 이슈

2.3.1 익명성(Anonymity)/필명(Pseudonym) 보안

효율적인 사물인터넷 서비스를 위해서는 대량의 이기종 데이터를 수집하고 수집된 데이터에서 의미를 추출해야 한다. 하지만 데이터를 수집할 때 누구로부터 데이터가 전송되었는지 알 수 있다는 단점이 있다[28]. 이러한 단점은 데이터를 제공하는 응답자에게 익명성을 제공하거나 필명을 사용함으로써 해결이 가능하다. Yang et al.은 N명의 응답자 중 t명을 대표들로 선택하여 응답자의 응답 메시지를 대표들의 공개키로 암호화하는 방법을 사용하였다[29]. Warner는 응답 데이터들을 통계적인 기법을 이용하여 데이터 분포를 재구성 하는 방법으로 랜덤한 응답 기법을 제안하였다[30].

이 밖에도 이기종 네트워크 사이에 익명 채널(Anonymous Channel)을 만들거나[31-35], k-익명화 메시지 전송 방법[36] 등을 이용하여 응답자의 프라이버시를 보호할 수 있다.

2.3.2 DB 보안 기술

사물인터넷은 이기종 네트워크에서부터 수집되는 데이터를 서비스에 맞는 형태로 가공하여 사용자에게 제공한다. 보안성을 위해서 데이터는 반드시 암호화하여 데이터베이스에 저장되어야 하지만 이는 데이터의 검색속도를 낮추어 서

비스 제공시 지연시간을 늘리는 원인을 제공한다. 특히 대용량의 데이터를 다루는 사물인터넷 서비스의 경우는 더욱 심각하다. 따라서 보안성을 제공하면서 데이터 검색을 빠르게 하여 신속하게 데이터 처리를 할 수 있는 암호 기술이 필요하다. 대표적인 기술로 검색 가능 암호 기술(Searchable Encryption Technique)이 있다[37]. 검색 가능 암호란 암호화된 자료를 복호화하지 않은 상태에서도 원하는 자료를 검색할 수 있게 해주는 기술이다. 이는 데이터 검색에 복호화가 필요하지 않기 때문에 빠르게 데이터에 접근할 수 있다는 장점이 있다.

검색 가능 암호 기술은 대칭키 기반 기술과 공개키 기반 기술로 나눈다. 대칭키 기반 검색 암호 기술은 데이터를 암호화 하여 저장한 상태에서 사용자만이 알고 있는 값을 아용하여 트랩도어를 만들고, 이 트랩도어와 암호문들을 사용하여 검색을 하는 방법으로 대표적인 기법으로, Goh의 Blomm filter를 사용한 방법[38], Golle의 conjuctive search 방법[39] 등이 있다. 공개키 기반 검색 암호 기술은 자신의 개인키로 트랩도어를 만들어 검색하는 기술로, Park의 공개키 기반에서의 conjuctive search 방법[40] 등이 있다.

2.4 데이터 처리 단계에서의 보안 이슈

2.4.1 Privacy preserving data mining

IoT 서비스는 데이터를 처리함에 있어서 프라이버시 침해 가능성이 높기 때문에 프라이버시 보호형 마이닝 기법(Privacy Preserving Data Mining)을 사용할 필요가 있다. 프라이버시 보호형 마이닝 기법은 4가지로 분류할 수 있는데, 첫 번째로 프라이버시 보존형 데이터 퍼블리싱 기법은 데이터 처리 및 가공 후, 그 결과 값이 프라이버시 침해가 되지 않도록 변형을 가하는 기법이다. 두 번째로 데이터마이닝 결과 변형 기법은, Association Rule Hiding과 같이 알고리즘 자체를 변형하는 방법이다. 세 번째로 쿼리 감사 기법은 쿼리 결과값을 수정하거나 제한하여 정보 누출을 방지한다. 마지막으로 분산프라이버시 기법은 Pinka의 multiparty 프로토콜과 같이 데이터 분산화를 통해 프라이버시를 보호한다.

2.5 서비스 영역에서의 보안 이슈

2.5.1 접근제어/권한 제어 기술

서비스 영역에서의 대표적인 보안이슈로는 서비스에 대한 접근제어가 있을 수 있다. 일반적인 환경에서 접근제어를 위해 주로 사용되는 기법으로는 임의적 접근제어(Discretionary Access Control), 강제적 접근제어(Mandatory Access Control), 역할기반 접근제어(Role-Based Access Control), 속성기반 접근제어(Attribute-Based Access Control) 기법으로 나뉘어진다. 이러한 접근제어 기법들을 사물인터넷 상의 서비스관점에서 보면, 임의적 접근제어는 서비스 제공자가 서비스 사용자에 대한 권한을 직접 부여할 수 있는 방식이 될 수 있다. 임의적 접근제어기법을 사물인터넷 서비스의 유연성에는 용이하지만, 서비스 제공자의 실수 및 고의로 인한 보안문제가 생길 수 있다. 강제적 접근제어 기법은 임의적 접근제어기법의 보안 문제를 보완하기 위하여, 서비스 제공자 대신에 공통플랫폼을 통해 IoT 관리자와 같은 최고 권한자가 서비스 사용자에 대한 권한을 설정하는 방식이다. 역할기반 접근제어는 비임의적 접근제어(Non DAC)로 분류되며, 서비스 사용자에게 각각 역할을 부여하고 특정역할마다 서비스에 대한 접근권한을 부여할 수 있는 방식으로 접근제어 작업을 단순화할 수 있다. 역할기반 접근제어기법은 요구사항

및 조건에 따라 Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, Dynamic Separation of Duty Relations로 나뉘어진다. 속성기반 접근제어기법은 사용자의 인증을 수행하고, 사용자의 권한이 아닌 속성에 따라 접근제어를 수행하는 기법이다. 속성기반 접근제어기법에서 사용되는 속성(attribute)에는 할당된 역할, 사용자 ID, 소속, 거주지 등의 정보가 될 수 있다. 이와같이 접근제어 주체와 방법에 따라 임의적/강제적 접근제어와 역할/속성기반 접근제어로 나누어 질 수 있다. 이뿐만 아니라 기밀성 또는 무결성과 같은 보호하고자 하는 요소에 따라서도 Bell-Lapadula 모델, Chinese Wall모델, Biba Integrity 모델, Clark-Wilson 모델 등이 있다. 사물인터넷에서의 서비스도 마찬가지로 접근제어를 수행하고자 하는 주체, 요소뿐만 아니라 기밀성이나 무결성에 대한 보안레벨을 평가하여 그에 맞는 접근제어기법을 적용할 필요가 있다.

2.5.2 공개 API 기술

공개 API(Open API)는 REST, SOAP과 같은 웹기반 기술을 사용하는 서비스를 접근하기 위한 공개된 API를 의미한다. 대표적인 공개 API로는 구글 지도가 있으며, 최근에는 Google외에도 Facebook, Twitter 등 대부분의 소셜 네트워크 서비스에서 사용되고 있다. 공개 API를 사용하기 위해서는 사용자 인증을 수행하는데, 초창기에는 웹에 등록된 사용자 아이디와 비밀번호를 사용하여 인증을 하였다. 그러나 트래픽분석에 의한 사용자 정보유출 문제가 부각되자 공개 API를 접근할 때 인증에 대해 관심을 가지기 시작했고, 이에 대한 해결방법으로 OpenID, SAML, OAuth등이 제안되었다. OpenID 방식은 ID를 제공해주는 3자 서비스를 통해서 OpenID를 인증받고 공개 API를 사용하는 기법이다. OpenID 방식에서는 사용자와 RP(relying party), OP(OpenID 제공자)가 참여하여 인증을 수행하게 된다. 인증 과정 중에 사용자는 RP를 통해서 OP로부터 OpenID를 인증 받는데, 이 같은 특징 때문에 OpenID방식은 악의적인 RP에 의한 피싱 공격이 가능하며, 2012년에 Wang et al.[41]에 의해서 위장공격에 대한 취약점이 알려졌다. SAML(Security Assertion Markup Language)은 OASIS에서 제안한 모델로 XML에 기반하며, 인증과 인가를 수행한다. SAML에서는 사용자, idP(ID 제공자), SP(서비스제공자)로 3개의 개체로 나누어지며, 사용자는 인증을 받기 위해서 SP로부터 받은 SAML 요청을 통해서 인증 및 인가를 수행한다. 2011년도에 Jager와 Somorovsky[42]에 의해서 XML signature wrapping에 대한 취약점이 발표된 바있다. OAuth 1.0[43] 인증 방식은 2010년에 RFC 5849로 처음 제안되었다. OpenID와 SAML 프로토콜은 SSO(Single Sign On)을 목표로 제안되었지만, OAuth는 공개 API에 대한 인가를 목표로 개발되었다. OAuth에서는 사용자, OAuth 제공자, OAuth 고객으로 나누어지며, 사용자가 API를 이용하기 위해서는 OAuth 고객인 서비스에 로그인을 하고 OAuth 고객은 OAuth 제공자에 요청토큰과 비밀키를 발급받고, 사용자는 해당 요청토큰과 비밀키를 인증받아 최종적으로 접근토큰(Access Token)을 획득한다. OAuth 1.0은 공격자가 인가된 사용자의 세션을 고정시키는 세션 고정공격에 대한 취약성을 가지고 있으며, 현재는 OAuth 2.0[44]이 제안되었으며, Google, Facebook, Twitter 등 공개 API를 사용하는 서비스에서 가장 보편적으로 사용되고 있다. OAuth 2.0은 서명, 암호화 등을 SSL에만 전적으로 의존하고 있으며, 구현관점에서 여전이 많은 보안문제를 가지고 있다. 이를

위해 OAuth 2.0에서 고려해야할 위협 및 보안 요소[45]를 RFC6819에서 제안하였다.

2.5.3 서비스 보안 기술

웹 서비스는 WSDL(Web Service Definition Language), UDDI (Universal Discovery and Integration of Business for Web), SOAP(Smple Object Access Protocol) 등 세 개의 표준으로 이루어진다.

특히 SOAP은 XML기반의 RPC(Remote Procedure Call) 프로토콜로, 실제 메시지 송수신의 핵심프로토콜이다. 안전한 웹 서비스를 제공하기 위해서는 SOAP 프로토콜 보안에 대한 고려가 필요하다. 대표적인 SOAP 보안으로는 OASIS에서 제안한 방법으로는 WS-Security(Web Services Security) 표준[46]을 필두로 SAML과 XACML이 있으며, 그 외에도 W3C에서 제안한 XML Signature/Encryption, XKMS 2.0[47], SOAP-SEC[48] 등이 있다.

2.5.4 ID 관리 기술

사물인터넷을 위한 서비스를 제공하기 위해서는 사용자 인증을 거쳐서 인가된 사용자에 대한 접근만 허용하여 가용성을 보장할 수 있어야 한다. 이를 위해서 가장 간단한 인증기법으로는 식별자(ID)를 통한 인증이 있다. 최근에는 정보통신의 발전으로 서비스 제공자가 관리해야하는 ID정보가 기하급수적으로 증가함에 따라 이러한 ID 관리 문제로 인한 개인정보 누출, 주민번호 도용 등의 문제가 발생하면서 사회적인 관심을 받고 있다. 따라서 ID 관리 문제를 해결하기 위한 연구를 국내외에서 진행 중이다. 특히 OpenID는 ID 관리를 위한 대체기술로 주목받고 있으며, URL 기반으로 인증을 수행한다. 대표적인 국내 ID관리 기술로는 한국전자통신연구원에서 개발한 CoT(Circle of Trust)를 이용한 e-IDMS(ETRI-Identity Management System)[49]가 있다.

3. 결 론

본 고에서는 센싱 기술과 정보 가공 기술, 저장 및 서비스 활용 기술의 융복합적 특성을 가지는 사물인터넷 서비스를 안전하고 신뢰할 수 만들기 위한 주요 보안 기술에 대해 살펴 봤다. 사물과 사람, 서비스가 하나의 공간으로 통합되어 사람을 위한 서비스를 수행하는 사물인터넷의 장점은 내재적 문제점인 보안 취약성과 프라이버시 침해 문제를 해결하지 않고는 그 의미가 퇴색될 수 밖에 없을 것이다. 본 고에서 제시된 사물인터넷 보안 기술은 분석 및 이해를 돕기 위해 디바이스 레벨과 디바이스간 통신/네트워크 레벨, 데이터 수집/보관/처리 단계, 서비스 레벨에서 분류하여 제시했지만, 사물인터넷에서는 이러한 단계별 필요 보안 기술 외에도 여러 단계가 통합적으로 연관성을 가지는 보안/프라이버시 보호 기술도 필요하다.

참 고 문 헌

[1] 지식경제부, “USN산업 발전 전략”, 2012.12.
[2] L. Fang, D. Gannon, F. Siebenlist, XPOLA—an extensible capability-based authorization infrastructure for grids, in: 4th Annual PKI R&D Workshop, April, 2005, pp. 30-40.
[3] N. Hardy, The Confused Deputy: (or why capabilities might have been invented), ACM SIGOPS Operating Systems Review 22 (4) (1988) 36-38.
[4] eXtensible access control markup language

version 3.0, OASIS XACML v. 3.0, August 2010

[5] H. Levy, Capability-Based Computer Systems, Digital Press, Bedford, Massachusetts, 1984. Available: http://www.cs.washington.edu/homes/levy/capabook/.

[6] A.S. Tanenbaum, S.J. Mullender, R. van Renesse, Using sparse capabilities in a distributed operating system, in: Proc. 6th Int. Conf. on Distributed Computing Systems, 1986, pp. 558–563. Available:ftp://ftp.cs.vu.nl/pub/papers/amoeba/dcs86.ps.Z.

[7] S. Gusmeroli, S. Piccione, D. Rotondi, A capability-based security approach to manage access control in the Internet of Things, Mathematical and Computer Modelling, vol. 58, no. 5-6, pp. 1189-1205, Sep. 2013

[8] J. L. Hernandez-Ramos, A. J. Jara, L. Marin, and A. F. Skarmeta, Distributed Capability-based Access Control for the Internet of Things, Journal of Interner Services and Information Security, vol. 3, no. 3/4, pp. 1-16, Nov. 2013

[9] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, Identity Authentication and Capability Based Access Control(IACAC) for the Internet of Things, Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309-348, 2013.

[10] Security-Enhanced Linux, http://www.nsa.gov/selinux.

[11] Windriver, “Security in the Internet of Things”, 2014.

[12] A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, “Present: An ultra-lightweight block cipher”, In *Proceedings of the International conference on Cryptographic Hardware and Embedded Systems(CHES 07)*, pp. 405-466, 2007.

[13] C. Cannière, O. Dunkelman, M. Knežević, Katan, and Ktantan - “A family of small and efficient hardware-oriented block ciphers”, In *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 09)*, pp. 272-288, 2009.

[14] D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, “The hummingbird-2 lightweight authenticated encryption algorithm”, In *Proceedings of the 7th International Conference on RFID Security and Privacy(RFIDSec'11)*, pp. 19-31, 2011.

[15] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, “Hight: a new block cipher suitable for low-resource device”, In *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems(CHES 06)*, pp. 46-59, 2006.

[16] Hong, D.; Lee, J.K.; Kim, D.C.; Kwon, D.; Ryu, G.H.; Lee, D. LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors. Proceedings of the 14th International Workshop on Information Security Applications, 2013, WISA ’13.

[17] J. P. Aumasson, L. Henzen, W. Meier, and M. N. Plasencia, “QUARK: a lightweight hash”, http:// 131002.net/quark, 2012.

[18] J. Guo, T. Peyrin, and A. Poschmann, “The photon family of lightweight hash functions”, in *Crypto 2011*, Lncs, vol. 6841, pp. 222-239, 2011.

[19] A. Bogdanov, M. Knežević, G. Leander, D. Toz, K. Varici, I. Verbauwhede, and Spongent: “The design space of lightweight cryptographic hashing”, http:// sites.google.com/site/spongenthash, 2012.

[20] M. Hell, T. Johansson, A. Maximov, and W.

Meler, “A stream cipher proposal: Grain-128”, In *IEEE International Symposium on Information Theory (ISIT 2006)*, 2006.
[21] J. Daemen, V. Rijmen, AES Proposal: Rijndael, NIST AES proposal, 1998.
[22] Wi-Fi Alliance, http://www.wi-fi.org
[23] ZigBee Alliance, http://www.zigbee.org
[24] Bluetooth, http://www.bluetooth.org
[25] Wikipedia, “Constrained Application Protocol,” Avilable at http://en.wikipedia.org/wiki/Constrained_Application_Protocol
[26] ETSI, “CoAP 3 & OMA Lightweight M2M,” Available at http://www.etsi.org/news-events/events/693-coap-oma-lightweight-m2m
[27] Allan Stockdill-Mander, “MQTT Security,” Available at https://www.oasis-open.org/committees/download.php/50161/X-MQTT-Security.txt
[28] Brickell, Justin, and Vitaly Shmatikov. “Efficient anonymity-preserving data collection.” Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2006.
[29] Yang, Zhiqiang, Sheng Zhong, and Rebecca N. Wright. “Anonymity-preserving data collection.” Proceedings of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining. ACM, 2005.
[30] Warner, Stanley L. “Randomized response: A survey technique for eliminating evasive answer bias.” Journal of the American Statistical Association 60.309 (1965): 63-69.
[31] D. Chaum. Untraceable electronic mail, return address and digital pseudonyms. Comm. ACM, 24(2):84-88, 1981.
[32] C. Park, K. Itoh, and K. Kurosawa. Effient anonymous channel and all/nothing election scheme. In Advances in Cryptology - Proceedings of EUROCRYPT 93, volume 765 of LNCS, pages 248-259. Springer-Verlag, 1993.
[33] K. Sako and J. Kilian. Receipt-free Mix-type voting schemes | a practical solution to the implementation of a voting booth. In Advances in Cryptology - Proceedings of EUROCRYPT 95, volume 921 of Lecture Notes in Computer Science, pages 393-403. Springer-Verlag, 1995.
[34] Markus Jakobsson. Flash mixing. In Proceedings of the Eighteenth Annual ACM Symposium on Principles of Distributed Computing, pages 83-89. ACM, 1999.
[35] P. Golle, S. Zhong, D. Boneh, M. Jakobsson, and A. Juels. Optimistic mixing for exit-polls. In Advances in Cryptology - ASIACRYPT 2002, volume 2501 of Lecture Notes in Computer Science, pages 451-465. Springer-Verlag, 2002.
[36] Luis von Ahn, Andrew Bortz, and Nicholas J. Hopper. k-anonymous message transmission. In Proc. 2003 ACM Conference on Computer and Communications Security, pages 122-130, Washington, DC, 2003.
[37] Abdalla, Michel, et al. “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions.” Journal of Cryptology 21.3 (2008): 350-391.
[38] E. J. Goh, “Secure Indexes,” Technical Report, 2003/216, IACR ePrint Crpytography Archive, 2003
[39] P. Golle, J. Staddon, and B. Waters, “Secure Conjunctive Keyword Search over Encrypted Data,” Applied Cryptography and Network Security Conference-ACNS, LNCS 3089, pp. 31-45, 2004.
[40] D. J. Park, K. H. Kim and P. J. Lee, “Public Key encryption with conjunctive field keyword search,” Workshop on Information Security Applications-WISA, LNCS 3325 pp.

73-86, 2004.
[41] Rui Wang, Shuo Chen, and XiaoFeng Wang. “Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services.” In Security and Privacy (SP), 2012 IEEE Symposium on, pp. 365-379. IEEE, 2012.
[42] Tibor Jager and Juraj Somorovsky. “How to break XML encryption.” In Proceedings of the 18th ACM conference on Computer and communications security, pp. 413-422. ACM, 2011.
[43] Eran Hammer-Lahav, “The oauth 1.0 protocol.” (2010).
[44] Dick Hardt, “The OAuth 2.0 authorization framework.” (2012).
[45] Torsten Lodderstedt, Mark McGloin, and Phil Hunt. “OAuth 2.0 threat model and security considerations.” (2013).
[46] Anthony Nadalin, Chris Kaler, Ronald Monzillo, and Phillip Hallam-Baker. “Web services security: SOAP message security 1.0 (WS-Security 2004).” Oasis Standard 200401 (2004): 1-20010502.
[47] Phillip M. Hallam-Baker and Warwick Ford. “XML Key Management Specification (XKMS).” In WWW Posters. 2001.
[48] Allen Brown, Barbara Fox, Satoshi Hada, Brian LaMacchia, and Hiroshi Maruyama. “SOAP security extensions: Digital signature.” See www. w3. org/TR/SOAP-dsig (2001).
[49] 최대선, 조상래, 김승현, 진승헌, 정교일, “인터넷 ID 관리 서비스”, 정보보호학회지, 18권, 4호, pp143-152, 2008년 8월

저 자 약 력

서 화 정

이메일 : hwajeong@pusan.ac.kr

- 2010년 2월 부산대학교 정보컴퓨터 공학부졸업(학사)
- 2012년 2월 부산대학교 컴퓨터공학과 졸업(석사)
- 2012년 2월~현재 부산대학교 컴퓨터공학과 박사과정 재학중
- 관심분야 : 사물인터넷, 정보보호, 타원곡선 암호

이 동 건

이메일 : guneez@pusan.ac.kr

- 2009년 2월 부산대학교 정보컴퓨터 공학부졸업(학사)
- 2011년 2월 부산대학교 컴퓨터공학과 졸업(석사)
- 2011년 2월~현재 부산대학교 컴퓨터공학과 박사과정 재학중
- 관심분야 : 사물인터넷, 정보보호, 부채널공격, 오류주입공격, VLSI Design

김 지 현

이메일 : jihyunkim@pusan.ac.kr

- 2010년 2월 부산대학교 정보컴퓨터 공학부졸업(학사)
- 2012년 8월 부산대학교 컴퓨터공학과 졸업(석사)
- 2011년 8월~현재 부산대학교 컴퓨터공학과 박사과정 재학중
- 관심분야 : 사물인터넷, 정보보호, 스마트그리드, 프라이버시 보안

김 호 원

이메일 : howonkim@pusan.ac.kr

- 1993년 2월 경북대학교 전자공학과학사
- 1995년 2월 포항공과대학교 전자전기공학과 공학석사
- 1999년 2월 포항공과대학교 전자전기공학과 공학박사
- 1998년~2008년 한국전자통신연구원(ETRI) 정보보호 연구단선임연구원/팀장
- 2008년~현재 부산대학교 정보컴퓨터공학부 부교수
- 관심분야 : 사물인터넷, 스마트그리드, 정보보호/프라이버시 보호 기술, 암호 칩, 임베디드시스템 보안

최 종 석

이메일 : jschoi85@pusan.ac.kr

- 2011년 2월 동명대학교 정보보호학과 졸업
- 2011년 3월~2013년 2월 부산대학교 컴퓨터공학과 석사과정
- 2013년 3월~현재 부산대학교 컴퓨터공학과 박사과정
- 관심분야 : 사물인터넷, 모바일 보안, 페어링 암호, 분산시스템 보안