IoT 환경에서 보안위협과 대응방안에 관한 연구

정현주, 이근호
백석대학교 정보통신학부
guswn4884@naver.com, root1004@bu.ac.kr

A Study of Security Threats and Countermeasures in IoT Environment

Hyun-Joo Jung, Keun-Ho Lee
Division of Information and Communication, Baek-Seok University

요 약

IoT (Internet of Things), 사물 인터넷은 인터넷을 기반으로 네트워크로 연결해 다양한 분야에서 사람과 사물, 사물과 사물 간의 정보를 공유하는 지능형 기술 및 서비스로 각 분석기관마다 2014년 10대 기술 중 하나로 꼽고 있다. 각국과 다수의 업체들이 사물인터넷 시장에 적극적으로 참여중이고, 관련 시장 규모도 급성장 할 것으로 전망하고 있다. 하지만 IoT의 빠른 발전과 함께 나타나는 것은 '보안'이라는 해결 과제이다. 실제로 IoT 사용에 따른 보안 위협이 발생하고 있다는 보고가 적지 않게 나오고 있고, IoT 환경의 보안은 아직 시작단계에 불과하다. IoT에서 발생하는 보안 위협의 형태의 대부분은 데이터 전송 그 자체에서 발생할 것이고, 데이터 전송에서 취약한 암호화나 인가되지 않은 주체로부터 접근, 보안이 취약한 네트워크 등에서 많은 보안 문제가 발생할 것이다. 본 논문에서는 IoT 기술의 개요와 IoT 환경에서의 보안위협에 대해 살펴보고 향후 연구의 방향을 제시하고자 한다.

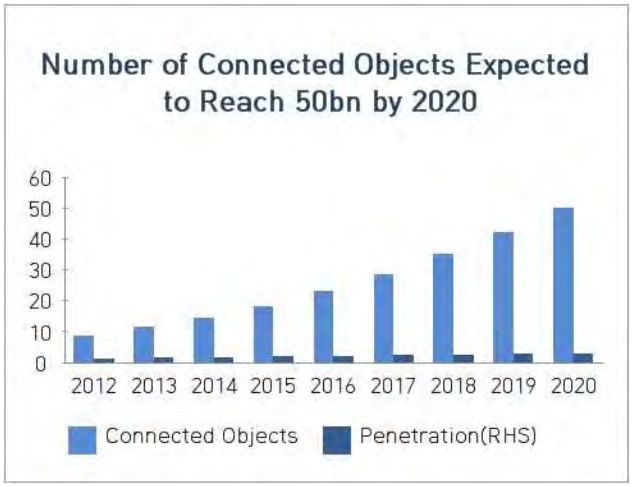
1. 서론

수년 전부터 IT 시장에서는 IoT가 주목을 받고 있다. IoT (Internet of Things), 사물 인터넷은 인터넷을 기반으로 네트워크로 연결해 다양한 분야에서 사람과 사물, 사물과 사물 간의 정보를 공유하는 지능형 기술 및 서비스로 각 분석기관마다 2014년 10대 기술 중 하나로 꼽고 있다. 특히 IT 시장조사기관인 가트너는 PC와 스마트폰을 제외한 인터넷 연결 기기가 2009년 9억대에서 2020년에는 약 260억대로 증가할 것으로 예상했고, 관련 시장규모 역시 급성장할 것으로 전망했다. 'CES 2014' 에서는 스마트 가전, 스마트 홈, 스마트 자동차 등의 사물 인터넷과 관련된 기술과 제품이 주로 전시되었다. IoT 기술을 이용해 에너지, 헬스케어, 자동차 등 사람을 위한 다양한 서비스 창출이 가능하다. 때문에 IBM, Apple, 삼성, LG, Google, HP, ERICSSON, BOSCH 등의 다수의 글로벌 업체들이 사물인터넷 시장에 적극적으로 참여 중이다.

미국은 국가정보위원회에서 사물 인터넷을 국가경쟁력 6대 혁신기술로 선정하여 기술개발 로드맵을 작성, EU는 제 7차 Framework Program의 일환으로 사물 인터넷 연구 프로젝트(CASAGRAS)를 추진 중이다. 중국은 사물인터넷에 대한 국가차원의 발전전략을 추진 중이고, 일본은 사물인터넷을 새로운 경쟁우위로 신사회 시스템 창출을 목표로 하고 있다. 한국도 정보통신전략위의 산하에 사물인터넷 기본 계획 등을 의결해 사물 인터넷 중심의 정책적 지원이 가속화될 가능성이 높다.

하지만 IoT의 빠른 발전과 함께 나타나는 것은 '보안'이라는 해결 과제이다. 실제로 IoT 사용에 따른 보안 위협이 발생하고 있다는 보고가 적지 않게 나오고 있다. IoT 기술은 비교적 최근에 나왔기 때문에 IoT 환경의 보안은 아직 시작단계에 불과하다.

본 논문에서는 IoT 기술의 개요와 IoT 환경에서의 보안위협에 대해 살펴보고 향후 연구의 방향을 제시하고자 한다[1,2,3].



(그림 1) 인터넷에 연결되는 기기의 수의 증가

2. 관련 연구

2.1 IoT 주요 구성 요소

IoT는 주요 구성 요소는 인간, 사물, 서비스이다. 인간은 IoT를 통해 사물, 서비스와 소통하며, 사물과 서비스도 IoT를 통해 서로 소통한다. 기존의 통신에서는 인간의 개입 하에 인간과 사물, 인간과 서비스 간의 관계가 형성됐지만, IoT를 통하면 사물과 서비스 간에 자체 통신이 가능하며, 사물과 사물, 서비스와 서비스 간의 연결을 가능하게 한다. <표 1>은 IoT 주요 구성 요소의 특성을 나타낸 것이다[4].

<표 1> IoT 주요 구성 요소의 특성

인간	- 독립적인 주체 - 사람, 사고, 행동 양식 등을 의미
사물	- 유형의 사물 (디바이스, 차량 등) - 무형의 사물 (It 서비스에서 특정 기능을 수행하는 가상 객체, 함수 등)
서비스	- 특정 목적을 위해 구현된 프로세스와 동작 메커니즘 집합을 의미 - 각종 IT 융합 서비스 (스마트 그리드, 물류, 보안관리, 교통 등)

2.2 IoT 주요 요소 기술

IoT는 센서/상황 인지기술, 통신/네트워킹 기술, 대량의 데이터를 처리하는 빅데이터 기술, 방대한 양의 데이터로부터 유용한 정보를 추출하는 데이터마이닝 기술, 사용자 중심의 응용 서비스 기술, 웹 서비스 기술, 보안/프라이버시 보호 기술 등의 다양한 형태의 기술을 필요로 한다. 그 중, 필수적인 주요 요소 기술로는 센싱 기술, 유무선 통신/네트워킹 기술, IoT 서비스 인터페이스 기술이 있다. 다음 <표 2>는 IoT의 주요 요소 기술을 정리한 것이다.

<표 2> IoT 주요 구성 요소 기술

센싱	- IoT 디바이스의 위치나 외부 환경 등을 센싱 - 동작인식센서, 환경감지센서, 생체측정센서 등의 다양한 센서 - 수집된 정보는 자체 처리하거나, 원격지에 있는 클라우드 또는 IoT 디바이스에 전송
네트워킹	- 인간과 사물, 서비스를 연결
서비스 인터페이스	- 인간, 사물, 서비스의 특정 기능을 수행하는 응용서비스와 연동하는 역할을 수행

센싱 기술은 온도, 습도, 열, 가스, 초음파, 동작 인식, 생체 측정 등 주위 환경과 유형 사물로부터 정보를 얻을 수 있는 물리적 센서와 가상 센싱 기능을 가진 기술이 있다. 이미 센싱한 데이터로부터 특정 정보를 추출하는 가상 센싱 기능은 실제 IoT 서비스 인터페이스에서 구현된다. 이를 통해 기존의 독립적인 물리적 센서보다 지능적이고 고차원적인 정보를 추출할 수 있다.

IoT의 유무선 통신 및 네트워크 장비로는 기존의 Wi-Fi, 3G/4G/LTE, Bluetooth, 위성통신, Microware, PLC 등 인간과 사물, 서비스를 연결시킬 수 있는 모든 유무선 네트워크를 의미한다. 디바이스 스스로가 수집한 정보를 필요에 따라 다른 디바이스와 커뮤니케이션하며 새로운 정보를 창출하기 위해서는 네트워크 서비스가 중요하다.

IoT 서비스 인터페이스는 정보를 센싱, 가공, 추출, 처리, 저장, 판단, 상황 인식, 인지, 보안, 인증, 인가, 오픈 플랫폼 기술, 미들웨어 기술, 데이터마이닝 기술, 웹 서비스 기술, 소셜 네트워크 등 서비스 수행을 위해 저장, 처리, 변환 등의 역할을 수행한다. 단순히 일차원적으로 센싱을 통한 정보를 추출하는 것과 다르게, 기존의 비 가공 데이터를 분류 및 가공, 처리함으로써 상황에 맞는 의미 있는 정보를 추출할 수 있는 기술이다[4].

3. 보안위협

IoT 기술은 단순히 인터넷으로 연결되는 사람과 사물을 말하는 것이 아니라, 인터넷에 연결되면서 어떤 새로운 서비스를 창출하는 것을 말한다. <표 3>은 IoT 구성요소에서 나타날 수 있는 보안 위협을 정리한 것으로, 수많은 IoT 기기들의 인터넷 연결이 지속적으로 증가하면서 디바이스와 네트워크, 창출되는 서비스에서 보안위협 역시 다양하게 나타나고 있다는 것을 보여주고 있다.

<표 3> IoT 구성요소에서 나타날 수 있는 보안위협

IoT 구성요소	보안위협
사물 (디바이스)	공통된 플랫폼 부재
	인증 수단의 부재
네트워크	무선 네트워크의 구조적 취약성
서비스	IoT 보안 기술 표준화의 부재

4. 대응방안

IoT 환경에서 예상되는 보안 위협에 대한 대응방안을 제안하고자한다.

- 무선 네트워크의 구조적 취약성 : 노트북이나 스마트폰에서도 무선 인터넷에 대한 보안 취약성은 끊임없이 제기된다. 사물인터넷의 특성상 인터넷과 같은 공공의 네트워크를 통해 데이터가 전송되기 때문에, 완벽한 무선 네트워크 보안의 표준을 제시해 안전한 네트워크 환경을 구축해야한다.

- IoT 디바이스의 공통된 플랫폼 부재 : 호환성 미흡으로 인해 서비스 업체별 호환성에 대한 문제 대두되고 있다. 공통된 플랫폼 이용 시 IoT기술을 활용한 어플리케이션의 개발이 쉽고, 보안 관리 등 전반적인 시스템 구축이 수월할 것이다. 공통 플랫폼 표준화를 추진하고, 서비스 플랫폼 개발, 구축을 적극 지원해야한다.

- 디바이스에 대한 인증 수단의 부재 : IoT 환경에서는 앞으로 스마트폰, 웨어러블 디바이스 등의 활용이 증가할 것으로 예상된다. 디바이스 인증에 대한 보안 인증기법에서도 여러 가지 위협이 존재하기 때문에 취약점을 분석하고 신뢰할 수 있는 디바이스만이 IoT 서비스를 안전하게 이용할 수 있는 적절한 디바이스 보안 인증 메커니즘이 필요하다.

- IoT 보안 기술 표준화 부재 : 현재 사물인터넷 시장의 선점을 위한 경쟁이 가속화되고 있고, 국제 표준 제정을 두고 각 연구기관과 표준화 기구의 주도권 경쟁이 일어나고 있다. 안전한 IoT 환경을 위해서는 이를 뒷받침할 IoT 보안 기술의 표준화, 보안 인프라 구축에 대한 연구가 필요할 것이다.

.

5. 결론

IoT에서 발생하는 보안 위협의 형태의 대부분은 데이터 전송 그 자체에서 발생할 것이고, 데이터 전송에서 취약한 암호화나 인가되지 않은 주체로부터 접근, 보안이 취약한 네트워크 등에서 많은 보안 문제가 발생할 것이다. 앞에서 짚었던 보안 위협에 관한 연구가 진행되어야 하며, 언급한 내용 외의 보안 위협을 해결하기 위한 대응방안과 IoT 보안 메커니즘에 관한 추가적인 연구가 필요하다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348). 또한 '산학협동재단'지원으로 수행된 연구임.

참고문헌

[1] 사물 인터넷(IoT) 기술에서 빼놓을 수 없는 것은 '보안', http://www.bdtinsights.com/kr/?p=1337

[2] 한국방송통신전파진흥원, 우리투자증권 투자정보부, "각국의 사물 인터넷 관련 정책"

[3] http://cafe.naver.com/morningasset/1899

[4] 김호원, 김동규, "IoT 기술과 보안", 한국정보보호학회, 2012