Journal of the Korea Convergence Society
Vol. 8. No. 9, pp. 1-7, 2017
https://doi.org/10.15207/JKCS.2017.8.9.001

시나리오 분석을 통한 사물인터넷(IoT)의 취약성 분석

홍성혁[1*], 신현준[2]
[1]백석대학교 정보통신학부, [2]목원대학교 융합컴퓨터미디어학부 컴퓨터공학과

Analysis of the Vulnerability of the IoT by the Scenario

Sunghyuck Hong[1*], Hyeon-Jun Sin[2]
[1]Div. of Information Communication, Baekseok University
[2]Division of Convergence & Media, Mokwon University

요 약 네트워크 환경의 개발과 고속화가 되면서 수많은 스마트 기기가 개발되고, 사람과 사물의 상호작용을 가능하게 하면서 고속화된 스마트사회를 구현할 수 있다. 사물인터넷의 수가 급증함에 따라 장치, 플랫폼 및 운영 체제, 통신 및 연결된 시스템에 대한 광범위한 새로운 보안 위험 및 문제점들이 부각되고 있다. 사물인터넷(Internet of Things)장비 들이 갖는 물리적인 특성상 기존 일반 시스템에 비해 크기가 작고 저전력, 저비용, 상대적으로 낮은 스펙으로 운용 제작되기 때문에 연산 및 처리 능력이 떨어져 기존 시스템에서 사용하던 보안 솔루션 적용에 한계가 있다. 또한 IoT(Internet of Things)기기들이 네트워크에 항상 연결되어 있는 특성에 따라 도청 및 데이터의 위·변조, 프라이버시 침해, 정보 유출, 비 인가된 접근, 루팅 및 업데이트 취약성 등 개인의 사생활 노출이나 국가의 중요 기밀과 시설에 대한 위협까지 중대한 보안상 문제들이 나타날 수 있다. 따라서 본 논문에서는 사물인터넷(IoT)의 네트워크의 보안위협사례와 피해사례를 조사하고, 취약성을 시나리오를 통해 분석하여 사물인터넷에 의한 재산피해 최소화하기 위한 방안을 제시하였으며, 시나리오를 이용하는 방법으로 취약점을 분석하였다.

• 주제어 : 사물인터넷, 사물인터넷(IoT) 취약성, 사물인터넷(IoT) 보안, 네트워크 보안, 취약점분석

Abstract As the network environment develops and speeds up, a lot of smart devices is developed, and a high-speed smart society can be realized while allowing people to interact with objects. As the number of things Internet has surged, a wide range of new security risks and problems have emerged for devices, platforms and operating systems, communications, and connected systems. Due to the physical characteristics of IoT devices, they are smaller in size than conventional systems, and operate with low power, low cost, and relatively low specifications. Therefore, it is difficult to apply the existing security solution used in the existing system. In addition, IoT devices are connected to the network at all times, it is important to ensure that personal privacy exposure, such as eavesdropping, data tampering, privacy breach, information leakage, unauthorized access, Significant security issues can arise, including confidentiality and threats to facilities. In this paper, we investigate cases of security threats and cases of network of IoT, analyze vulnerabilities, and suggest ways to minimize property damage by Internet of things.

• Key Words : Internet-of-Thing (IoT), IoT Vulnerability, IoT Security, Network Security, Security Analysis

*Corresponding Author : 홍성혁(shong@bu.ac.kr)
Received July 11, 2017 Revised August 18, 2017
Accepted September 20, 2017 Published September 28, 2017

1. 서론

1.1 IoT사물인터넷(Internet of Things)

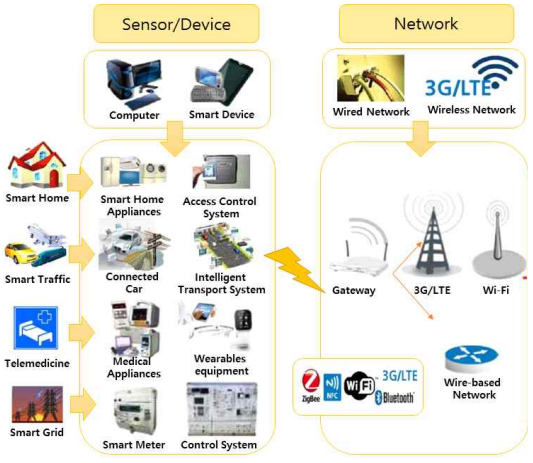
IoT사물인터넷(Internet of Things)은 사용자 제어에 의하여 작동하는 스마트기기부터 사용자의 제어가 없이도 스스로 작동하는 센서를 포함한 모든 기기들이 네트워크를 통하여 상호통신 할 수 있도록 하는 기술이다[1]. 기존 사물인터넷의 형태는 사물과 사물간 통신(Machine to machine, Mto(2)M)으로 이기기 중심의 하드웨어적 접근이었다면, 최근 IoT사물인터넷(Internet of Things, IoT)기기들은 소프트웨어와 사용자의 서비스 중심의 접근이라 할 수 있다[2]. Fig. 2.를 통해 기존 시스템과 IoT 사물인터넷(Internet of Things)기기의 차이를 보여주고 있다[3].

사물(Things)의 센서들이 만들어낸 정보가 네트워크를 통해 공유하는 환경으로 모바일기기의 네트워크 보다 진보한 단계의 인터넷을 의미한다[4]. 지금도 매순간 새로운 기술이 개발되고, 기존의 기술들이 또 다른 새로운 기술과 융합되면서 전혀 다른 기술로 발전 되고 있다. 특히 새로운 기술들이 매우 빠른 속도로 확산되면서 사람과 사물, 사물과 서비스 등이 밀접하게 연결되면서 더욱 더 강력한 디지털 생태계가 만들어지고 있다. 즉, IoT사물인터넷(Internet of Things)기기들이 급증함에 따라 세상의 모든 사물을 연결하는 초 연결 사회(Hyper Connect Society)라는 말까지 생길정도로 IoT사물인터넷(Internet Of Thing)보급이 빨라졌고, 세계는 IoT사물인터넷(Internet Of Thing)시대로 도래하고 있다. 가트너 선정 년도 대 전략기술 2015 '10 IT '(Top10 Strategic IT Trends) (2013:사물인터넷 위 만물인터넷 위 사물인터넷 위 로 선정된 기술의 발달은 사물과 사물의 상호작용은 물론 사람과 사물사이의 상호작용을 가능하게 하고 생활을 스마트하고 편리하게 만들고 있다 실제로도 LG U+와 KT에서 IoT Home 서비스상품과 기기들을 출시하는 등 집 안에 있는 난방, 전기 스위치, 현관문 도어락 같은 보안기기 사물들을 인터넷으로 연결하여 시공간을 초월하여 내부 상태를 확인할 수 있게 서비스 하고 있다[5]. IoT Home 서비스는 사물인터넷(Internet of Things, IoT)기기들이 홈네트워크 연결되면서 가정환경과 사람의 자연스러운 상호작용뿐만 아니라 가전제품이나 주변 센서와 데이터 송수신을 통해 정보 교류, 모니터링 사람이 일일이 제어하지 않아도 첨단 기능을 자동으로 조절 제어를 도와준다. 또한 네트워크 공유기를 통해 사용자는 집 외부에서 컴퓨터나 휴대전화 어플로 가스나 전자제품을 끄고 켤 수 있고, 교육・영화・게임 등의 멀티미디어 자료를 쉽게 접할 수 있다. 인간의 삶의 질을 보다 향상시키고 편안한 가정환경을 누릴 수 있게끔 도와준다[6].

사물인터넷에 활용 범위가 넓어 Table 1과 같이 그 수가 2018년에는 IoT 사물인터넷(Internet of Things)이 휴대전화 가입자 수를 넘어설 것이라고 판단한고 있다 [7]. 또 시장조사기관인 가트너(Gartner)보고서에 의하면 세계 인터넷 접속 기기가 오는 2020년까지 250~300억대이상으로 증가할 것이라고 전망하고 있다[8]. 인터넷 접속 기기의 증가는 IoT 서비스(IoT services)와 사물인터넷(Internet of Things, IoT) 디바이스의 증가가 주요 원인이다. [Fig. 1]은 인테넷과 현재 사용 중인 센서 네트워크와의 차이를 보여준다.

<Table 1> Internet of Things Installed Base Will Grow

	2015 (15billion)	2021 (28billion)	CAGR 2015-2021
Cellular IoT	0.4	1.5	27%
Non-cellular IoT	4.2	14.2	22%
PC/laptop/tablet	1.7	1.8	1%
Mobile phones	7.1	8.6	3%
Fixed phones	1.3	1.4	0%



[Fig. 1] The difference between the Internet and the existing system.

1.2 사물인터넷(Internet of Things, IoT)의 취약성

사물인터넷이 가지고 있는 대표적인 특성을 크게 두 가지로 분류하고 분석해 보았다. 먼저 사물인터넷

(Internet of Things, IoT)장비들이 항상 네트워크상에 연결되어 있는 구조적인 특성상 도청, 무선신호 교란, 정보 유출, 비 인가된 접근, 데이터 위·변조, 서비스 거부, 루팅 및 업데이트의 취약성 등 네트워크를 통한 보안상의 문제점들이 주를 이루고 있다. 장비 해킹으로 인한 보안위협으로, 개인의 사생활 국가의 중요 기밀과 시설에 대한 위협까지 중대한 보안상 위협들이 나타날 수 있다. 다음으로 사물인터넷(Internet of Things, IoT)장비 들이 갖는 물리적인 특성상 기존 일반 시스템에 비해 크기가 작고 저전력, 저비용, 상대적으로 낮은 스펙으로 운용 제작되기 때문에 연산 및 처리 능력이 단순하다. 때문에 기존 시스템에서 사용하던 기성 보안 솔루션이나 소프트웨어를 적용하기가 어렵다는 문제가 있다. 기존 PC나 모바일폰처럼 사용자가 스스로 보안프로그램을 설치하여 운용하거나 보안 정책을 직접 설정하기가 어렵고 일반 사용자들은 IoT(Internet of Things)기기 내부에 접근할 수 없기 때문에 사용자 개인에 의한 보안 정책이나 소프트웨어 설치가 어렵다는 점도 문제가 될 수 있다. 이와 같이 일반 사용자 입장에서는 구입 이후에 비밀번호 설정을 제외한 보안 업데이트 적용 등 제작사의 보안 패치를 통해 보다 안전한 서비스를 기대할 수 있다 [9].

사물인터넷은 가치와 잠재력이 무궁무진 하다. 때문에 사물인터넷이 미치는 영향력과 기능이 커지고 우리의 삶에 더욱더 가까워질수록 보안문제에 대한 위협이 사이버 공간에서 끝나는게 아니라 실제 물리적인 시스템에 의한 피해로 크기가 증가한다. 다양한 보안 위협으로 부터 사물인터넷(Internet of Things, IoT) 장비들은 수많은 공격자로 부터의 해킹 위험성이 높아지고 있다.

본 연구에서 IoT(Internet of Things) 기기들의 취약성에 대한 사례를 조사하고 문제점을 분석하여 보안 위협을 예방하기 위한 방법을 연구한다.

2. IoT사물인터넷(Internet of Things) 취약성 사례 분석

2.1 국내 사례분석

요즘 지어지는 모든 아파트에는 [Fig. 2]와 같이 스마트 월패드가 기본적으로 설치되어있다. 월패드를 해킹해 외부에서 보내는 패킷을 마치 실내에서 조작하는 것처럼 위조해 외부에서 네트워크를 통해 집안에 있는 전등을 조작하거나 가스, 보일러 등 심지어 현관문까지 열고 집에 침입할 수 있다.

[Fig. 2] Image of Wall-Pad

융합제품이나 융합서비스를 활용하는 IoT(Internet of Things, IoT)기기 70%가 암호화되지 않은 네트워크를 통해서 전송하는 것으로 파악 됐다. 또한 원격 관리 서비스가 열려있고, 제작사 별로 동일한 계정 정보를 사용하는 등 아파트 한 세대의 정보를 알면 전 세대에 접근이 가능할 수 있는 것으로 나타났다.

2.2 국외 침해사례

호주의 한 호텔에서 객실 문을 제어하는 시스템이 랜섬웨어에 감염되는 사례가 있다. 이 호텔은 당장 객실 문을 열 수 없게 되면서 고객들이 큰 불편을 호소하자 호텔 측은 해커에게 수백만원을 지불했다.

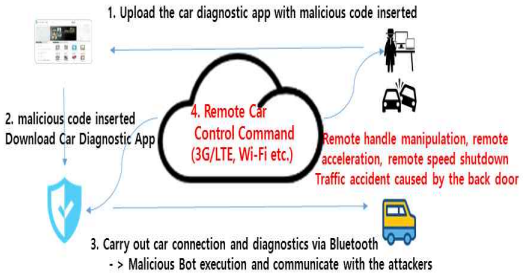
최근 국내에서는 자동차가 원격으로 해킹되는 사례가 방송되면서 자동차도 랜섬웨어나 해킹에 자유롭지 못한 것을 인식하게 되었다. 자동차가 랜섬웨어에 감염되면 운전자는 자동차 제어권을 돌려받기 위해 금전을 지불해야 한다. 해커가 자동차라는 재화이자 이동 수단을 인질로 잡는 셈이다. 더 악의적인 경우로는 운전자의 생명까지 인질로 잡을 가능성도 배제할 수 없다. 자연스럽게 해커가 요구하는 금전의 액수도 커질 전망이다.

예전에는 랜섬웨어의 목적이 단순히 좀비PC를 만들거나 사용자의 개인정보를 빼앗아가는 것이 아니다. 금전의 요구나 신체적 피해 심하게는 생명에 위협까지, 물리적인 피해로 번질 수 있는 것으로 나타났다.

2.3 기타 IoT(Internet of Things)취약성 시나리오 분석

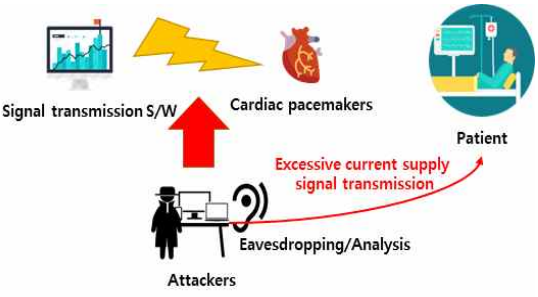
본 연구의 차별성은 단순 나열이 아닌 시나리오 분석을 통하여 구체적인 사례를 제시하여 독자가 쉽게 이해할 수 있도록 본문을 구성하였다.

Flg. 3부터 7은 IoT사물인터넷 기기가 해킹을 당할 수 있는 시나리오를 분석한 것이다[10]. IoT(Internet of Things)서비스 환경에서 보안취약점을 이용한 5가지 시나리오 사례를 보여주고 있다. 요즘 최근 국내에서 대두되고 있는 스마트카에 관한 차량진단, 의료기기에 관련된 심박기 신호위·변조, 국내 통신사에서 앞다퉈 출시하고 있는 스마트 홈 IoT(Internet of Things, IoT)의 원격조정, 교통정보 신호제어, 항공기제어시스템 오동작시나리오의 피해 사례가 있다.



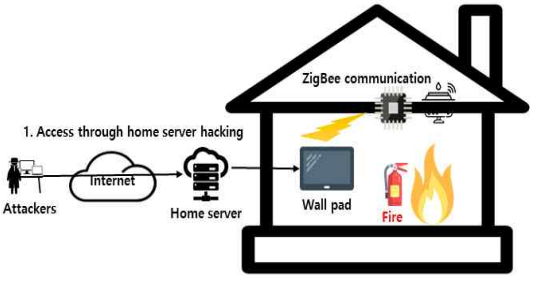
[Fig. 3] Vehicle remote control via a vehicle diagnostic app with malicious code

Fig. 4는 해커가 악성코드가 삽입된 차량진단 어플리케이션(Application)을 배포하면 사용자는 악성코드가 삽입되어있는 어플리케이션(Application)을 다운로드하게 되고 차량의 블루투스 및 차량의 USB를 통한 통신을 통해 진단수행을 하게 된다. 휴대폰을 통해 전송된 악성코드는 해커의 명령에 따라 자동차를 원격제어 하여 핸들조작, 급가속, 급정지 등으로 공격자에 임의의 조작을 통해 교통사고를 유발시킬 수 있다.



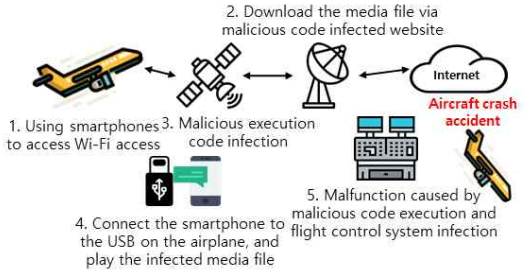
[Fig. 4] AED Over current flow through signal information and modulation

Fig. 5는 의료기기의 일부인 심박기를 예를 들고 있다. 심박기 신호를 위·변조해서 과전류를 흘려 환자에게 상해를 가하는 시나리오를 보여주고 있다. 심박기 신호정보를 관리하는 소프트웨어를 도청, 분석하여 원격에서 심박기의 전류량, 전원 등 작동을 마음대로 조작하여 심하면 환자의 생명까지 위협할 수 있다.



[Fig. 5] Remote opening of home gas valve via hacking of home servers

Fig. 5은 공격자가 외부 인터넷을 이용해서 홈 서버 해킹을 해킹하고, 원격지에서 댁내 가스밸브를 원격으로 개방하는 시나리오이다. 요즘 설치되는 월패드는 네트워크에 접속되면서 홈 네트워크의 중추 역할을 하고 있다. 시나리오에는 가스밸브로 예시를 들었지만 가스밸브 외에도 전기, 실내온도, 현관문까지 원격으로 조작이 가능하다. 요금으로 인한 금전적 피해나 화제, 무단침입 등 2차 3차 피해로 이어질 수 있다.



[Fig. 6] Harmful code infection and aircraft control system malfunction via in-flight Wi-Fi

Fig. 6은 비행기 안에서 제공하는 와이파이(Wi-Fi) 시스템을 통한 악성코드 감염을 통한 항공기 조작시스템 감염, 제어시스템의 오작동을 유발하는 시나리오이다. 비행기에 탑승한 승객이 노트북이나 스마트폰을 이용하기 위해 기내 와이파이(Wi-Fi)에 접속을 하게 된다. 기내 와이파이를 이용해서 웹서핑을 하거나 다운로드를 할 때 악성코드에 감염된 파일을 다운받게 된다. 사용자는 멀

티미디어 자료를 이용하기 위해 비행기에 준비된 USB에 악성코드자료를 전송하게 된다. 이 때 연결된 USB를 통해 비행기 내부 시스템에 악성코드가 감염되며, 비행기 제어시스템까지 통제 할 수 있게 된다. 제어시스템이 악성코드에 감염 되면 비행기 운항에 장애가 될 수 있고, 심각한 위험에 빠질 가능성도 있다[11].

위 보안위협 시나리오처럼 IoT(Internet of Things, IoT)가 우리 실생활에서 사용되는 사물에 적용되기 때문에 기존 사이버 공간에서 끝날 위험이 현신세계로 확대되서 나타날 수 있다. 한 국가의 IoT(Internet of Things, IoT)기간망의 취약점을 통하여 국가전체시스템을 마비시킬 수 있는 상태로 유발한다[12].

3. 사물인터넷(Internet of Things, IoT) 취약성에 대한 방안

3.1 하드웨어 중심의 데이터 암호화

IoT(Internet of Things)기기들을 절도, 화제, 자연재해 등과 같은 물리적인 취약성으로부터 보호하는 방법은 쉽게 설계, 적용할 수 있다. 하지만 도청 및 통신 위조를 통한 데이터의 위・변조 같은 네트워크 통신 신호를 교란하는 장비를 이용, 불법 무선통신 신호를 보내 통신 중인 데이터 또는 명령을 탈취해서 정상기기와의 통신처럼 위장하는 네트워크 보안 취약성이 있다. IoT(Internet of Things)기기들은 일반 시스템에 비해 상대적으로 초경량, 초저전력, 저 사양으로 제작이 된다. 이때 IoT기기를 장시간 작동시키기 위해 요구되는 시스템 파워를 최소화하는 경우가 많다. 때문에 시스템 프로그램에서 전력을 가장 많이 소모하는 보안 알고리즘을 탑재하지 않는 경우가 대부분이고, 소프트웨어를 통한 보안 솔루션 적용이 힘들다. 따라서 하드웨어에서의 데이터 암호화를 통해 공격자들의 공격을 차단하고, 시큐어 코딩을 통한 보안 알고리즘에 대한 전력 소모를 최소화 할 수 있도록 한다.

3.2 출시 전 보안 진단

IoT(Internet of Things)기기들은 제품이 발매되고 나면 사후 보안조치가 불가능 하거나 비용이 많이 드는 단점이 있다. 또한 사용자 입장에서 기기 내부를 쉽게 접근하기가 어렵기 때문에 임의의 보안 솔루션을 적용하기가 어렵다. 또한 보안 취약성이 사전에 개선되지 않는다면 서비스를 제공하는 회사는 제품 출시를 미뤄서 생기는 손실과 출시이후 생길 수 있는 문제에 대한 손해배상 등으로 금전적인 손실이 발생 할 수도 있다. 기업에서는 제품 출시 전에 취약성을 분석하고 없애는 노력을 기울여야 한다. 또한 주기적인 펌웨어 업데이트로 제로데이 취약성을 없애도록 노력해야 한다.

3.3 국가적 차원의 정책 수립

미국의 경우 헬스케어나 의료서비스와 같은 사람의 생명과 건강에 밀접하게 연관된 분야에서는 사물인터넷과 별도로 강력한 보안 지침을 규정해 이미 이를 의무화한 상태이다[13,14]. 한국 같은 경우에는 주요 IoT 인프라 보안 강화에만 신경을 쓰고 있다. 정보통신기반시설에 대한 신규 지정 및 보호체계만을 강화하고 있는 실정이다. 또한 이용자의 프라이버시 보호에 관한 정책과 기술만 주로 추진하고 있다 [15,16].

IoT 기기는 오픈소스를 주로 이용해서 제작되고 있다. 때문에 수많은 취약점이 발견되고 있다. 취약점들은 같은 오픈소스를 기반으로 하는 기기들에서 비슷한 유형의 취약성이 발견되고 있다. 사람의 생명까지도 위협받을 수 있는 IoT(Internet of Things)기기들을 국가적 차원에서 보안 모델의 기준을 계획하고 기준에 미달되는 기기의 경우에는 출시를 제한하도록 하는 등의 강력한 규제가 필요하다.

4. 결론

사물인터넷(Internet of Things)은 단말기 계층, 네트워크 계층, 서비스 계층으로 크게 세 부분으로 나눌 수 있다. 첫 번째로 단말부분의 보안 기술이다. 단말 장치간의 상호 통신이나, 센서와 통신이 이루어질 때는 통신의 유효성을 판단하게 되는데 이때 주로 사용되는 방식이 ID와 PW의 인증과 최근에는 지문, 홍채를 통한 생체인증 방식을 사용하는 경우도 있다. 하지만 생체인식을 통한 인증이 아무리 보안성이 뛰어나다고 해도 네트워크에 연결되어 있는 사물인터넷의 경우에는 통신 도중 인증데이터를 중간에서 탈취나 해킹에 의해서 외부에 노출 될 수 있다. 데이터가 노출되더라도 사용할 수 없도록 암호화를 꼭 해야 하고, 인증 정보에 세션정보를 적용시켜 일정기간이 되면 인증서를 만료시켜 사용자가 모르는 인증

데이터를 유지하지 않도록 해야겠다.

두 번째는 네트워크 계층이다. 사물인터넷은 다른 단말과의 연결을 위해 네트워크에 항상 연결되어있고, 수많은 데이터의 전송이 이루어질 뿐만 아니라 누구나 접근이 가능한 영역이다. 따라서 내부영역처럼 사용자들의 개인적인 네트워크영역과 외부 네트워크를 연결하는 게이트웨이의 보안은 필수적이다. 관리자 계정과 패스워드를 좀 더 어려운 패턴으로 지정하고, 게이트웨이 내부에서 단말간의 통신을 제외한 외부의 접근 패킷은 사용자가 지정한 출발지 호스트의 패킷만을 받아들일 수 있도록 필터를 설정해야한다.

세 번째는 플랫폼 서비스계층이다. 플랫폼의 형태도 과거에 비해서 사용자의 편이를 위한 쪽으로 많이 발전해 왔다. 현재는 PC나 모바일 그 외 단말기들은 동일한 플랫폼을 사용하고 있다. 때문에 PC에서 IoT기기를 침해할 수 있다. 플랫폼을 PC와 IoT장비 영역을 서로 분리시켜 구성하고, 이기종 간의 데이터 통신 사이에 방화벽을 설치하여 비인가 접근을 사전에 차단할 수 있도록 한다.

기업과 사회는 보안에 대한 관심 및 투자가 기술계발에 대한 투자와 관심에 비해 적은 것이 사실이다. IoT(Internet of Things)기기 에서의 보안은 개인 정보의 노출과 단순히 금전적 피해에서 멈추는 것이 아니라 이용자의 생명과 직결되는 제어에 관한 통신이 이뤄지기 때문에 보안 기술의 탑재와 적용은 필수적이다. 향후 생명과 직접적인 관련이 있는 사물인터넷은 별도의 인증체계를 구축하여 인증기준을 통과한 장비만 사용할 수 있는 기준을 향후 연구에서 할 예정이다.

ACKNOWLEDGMENTS

이 논문은 2017년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2017R1A2B1003394).

REFERENCES

[1] J. H. Kim, J. Y. Go, K. H. Lee, "A Scheme of Social Engineering Attacks and Countermeasures Using Big Data based Conversion Voice Phishing", Korea Convergence Society, Vol. 6, No. 1, pp. 85-92, 2015.

[2] B. Lee, W. S. Han. S. J. Kim, "Device Personalization Methods for Enhancing Packet Delay in Small-cells based Internet of Things," Dec 2016.

[3] M. J. Lee, "A Game Design for IoT environment", Journal of the Korea Convergence Society, Vol. 6, No. 4, 133-138, August 2015

[4] M. K. Sik, H. W. Park, "Global Trends discussion on privacy in the IoT environment, Institute for Information & communications Technology Promotion," pp. 12-23, June 2015.

[5] Y. S. Jeong, K. H. Han, S. H. Lee, "Access Control Protocol for Privacy Guarantee of Patient in Emergency Environment", The Journal of Digital Convergence, Vol. 12, No. 7, pp. 279-284, 2014.

[6] W. S. Bae, "Mutual authentication and Formal Verification in M2M Environment", The Journal of Digital Convergence, Vol. 12, No. 09, pp. 219-224, 2014.

[7] P. D. Drobintsev, V. P. Kotlyarov, I. G. Chernorutsky, L. P. Kotlyarova and O. V. Aleksandrova, "Approach to adaptive control of technological manufacturing processes of IoT metalworking workshop," 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), Saint Petersburg, Russia, pp. 174-176, 2017.

[8] C. J. Chae, H. J. Cho, "Smart Fusion Agriculture based on Internet of Thing", Journal of the Korea Convergence Society, Vol. 7. No. 6, pp. 49-54, 2016.

[9] Ciokorea, "Revenge·Theft·Peep… Smart Home Network is the New 'World of Hacking'," http://www.ciokorea.com/news/24723, 2015. 04.

[10] J. Pacheco, S. Satam, S. Hariri, C. Grijalva and H. Berkenbrock, "IoT Security Development Framework for building trustworthy Smart car services," 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, pp.

237-242. 2016.

[11] Ministry of Science, ICT and Future Planning, "Internet of Things-Information Protection Roadmap," 2014.

[12] K. B. Kim, H. J. Cho, "Regulation Improvement Measures for Activation of Internet of Things and Big Data Convergence", Journal of the Korea Convergence Society, Vol. 8, No. 5, pp. 29-35, May 2017.

[13] B. C. Kim, "A Internet of Things(IoT) based exploration robot design for remote control and monitoring", Journal of digital Convergence, Vol. 13, No. 1, pp. 185-190, 2015.

[14] J. Pacheco, S. Satam, S. Hariri, C. Grijalva and H. Berkenbrock, "IoT Security Development Framework for building trustworthy Smart car services," 2016 IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, pp. 237-242, 2016.

[15] B. Javed, M. W. Iqbal and H. Abbas, "Internet of things (IoT) design considerations for developers and manufacturers," 2017 IEEE International Conference on Communications Workshops (ICC Workshops), Paris, France, pp. 834-839, 2017.

[16] J. Rivera, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020" retried from http://www.gartner.com/newsroom/id/2636073, July, 2017.

저자소개

홍 성 혁(Sunghyuck Hong) [정회원]

- 1995년 2월 : 명지대학교 컴퓨터공학과 (공학사)
- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2007년 9월 ~ 2012년 2월 : Texas Tech University, Office of International Affairs, Senior Programmer
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수

<관심분야> : Network Security, Hacking, Secure Sensor Networks

신 현 준(Hyeon-Jun Sin) [학생회원]

- 2014년 3월 ~ 현재 : 목원대학교 2학년 재학

<관심분야> : Computer science, Reverse engineering, Network