Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Proposal and Analysis on the Security Requirements of the Hyper-Connected Society

Seong-Jong Kim*

Department of Ubiquitous IT, Far-East University

ABSTRACT

Smart society with convergences of technology and production comes, innovations of technology and production are expected to prevail everywhere. Also, a modern society is in a age of 'Internet of Things(IOT) and 'Internet of Everything(IOE)', which exchanges information among objects, via Internet, and it is expectable that the field of Internet of Things(IOT) will become a new-growth engine industry. However, as the interconnections among things are expanded, security threats are expected to be increased highly. Also, as the number of devices that require security increases and as the devices are enlarging their field to lightweight, low-power, hyper-connected and etc, the device-security technologies customized for each of the devices are needed in this stage. In this paper, I consider to Security Threat three part of Industry fields, Devices, Network and Flatform/Service. Therefore, by analyzing the security requirements for Internet of Things(IOT) in this thesis, the analysis is expected to be utilized for the countermeasures against security threats that can attack Internet of Things(IOT) in future. And as the expanded to Internet of Everything(IOE), the new security threat to security requirements that can respond to the threat analysis and developing technology are constantly will made to future.

KEYWORDS: Internet of things, Security requirements, Information and communications technologies, Hyper connected society, Internet of everything, Security threat

ARTICLE INFO: Received 26 June 2016, Revised 12 August 2016, Accepted 12 August 2016.

*Author is the Department of Ubiquitous IT, Far-East University, 76-32 Daehak-Gil Gamgok-myeon, Eumseong-gun, Chung-buk, Korea

E-mail address: ksj@kdu.ac.kr

1. 서 론

1-1 연구의 필요성

현대 사회는 사물들 사이에 인터넷으로 연결되어 정보를 주고받는 사물 인터넷(IoT ; Internet of Things) 시대이며, 사물 인터넷 분야는 신성장 동력 산업이 될 것으로 전망되고 있다. 사물 인터넷이 주목을 받는 이유는 다양한 산업과의 융복합을 통해 서비스 시장이 날로 커지고 있다는 점이다.

사회의 사물 인터넷 시대로의 급격한 이동은 시장 수요의 빠른 증가를 불렀으며 시장의 규모 또한 급격히 커져 2022년경에는 약 1조 2000억에 달할 것으로 예측되며, 사물 인터넷을 시대를 구축하기 위해 필요한 각종 장비 또한 기하급수적으로 증가할 것으로 예측되고 있다[1]. 하지만 사물 간 상호연결이 확대되면서 이에 따른 보안위협 역시 크게 증가할 것으로 예상되며, 보호해야 할 기기들의 수가 늘어나면서 그 특성도 경량화, 저전력화, 초연결성 등으로 다양화 되면서 기기별 맞춤형 디바이스 보안기술이 요구되고 있는 시점이라 할 수 있다. 또한 자율주행 자동차, 드론, 인공지능 로봇 등 미래 사회를 이끌어 나가게 될 산업 분야에 대하여 서는 발생 가능한 보안 위협들을 단계별로 분류하여 대처할 필요가 있다고 사료되며 표준화 작업도 시급히 병행해야 할 과제라 생각된다.

1-2 관련시장 동향

최근 창조경제의 기반 산업인 ICT(Information and Communications Technologies) 분야가 고도로 성장하면서 사물들이 통신망으로 유용한 정보를 주고받으며 필요한 정보를 처리하는 시대로 급격히 발전하고 있다. 궁극적으로는 사람과 필요한 모든 사물 그리고 네트워크가 하나로 연동되는 초-연결 사회(Hyper- Connected Society)로 변화할 것이 자명해지고 있다. IoT는 초-연결 사회를 구축하기 위한 핵심 기술로 부각 되었으며, 필요한 모든 것들이 연결될 만물 인터넷(IoE ; Internet of Everythings) 세상으로의 발전을 이끌게 될 것이다[2][3].

경제 분야는 오늘날 스마트 사회를 이끌고 있는 모바일 관련 산업이 무거운 연결과 운영체제 그리고 앱을 통한 경제가 중심이라면, 진화한 IoT 사회는 가벼운 연결이 중심이 되며 API(Application Programming Interface) 그리고 웹을 통한 경제로 변화될 것으로 전망된다[4]. 네트워크 장비 관련 산업계의 주요한 기업인 시스코(Cisco)의 보고서에 의하면, <그림 1>에서 나타내었듯이 앞으로 2020년까지 10년 동안 인터넷 연결에 필요한 장비의 수는 약 3.5배 이상 증가할 것으로 예측될 만큼 IoT 시대로의 변화는 피할 수 없을 것이며 이에 따른 대비도 시급한 것으로 보인다.

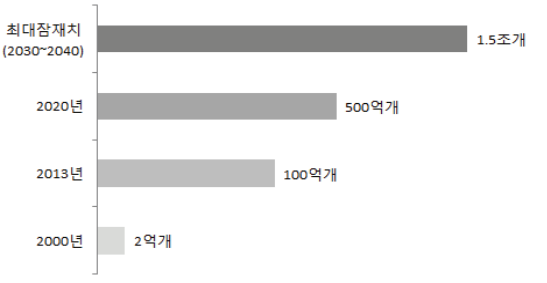

그림 1. 인터넷 연결 사물의 수
Figure 1. The number of things connected internet

또한 IoT 사회를 위한 경제 규모는 2022년까지 약 6 배가량 커질 것이며, 각 산업 분야별로는 그림 2와 같이 크게 장비 산업(37.2%), 시스템 산업(29.8%), 애플리케이션/서비스 산업(29.7%)이 전체의 96.7%를 차지할 것으로 보이는 만큼 기존 네트

워크 산업에 더하여 해당 산업에 대한 지원과 연구 개발이 절실할 것이다.

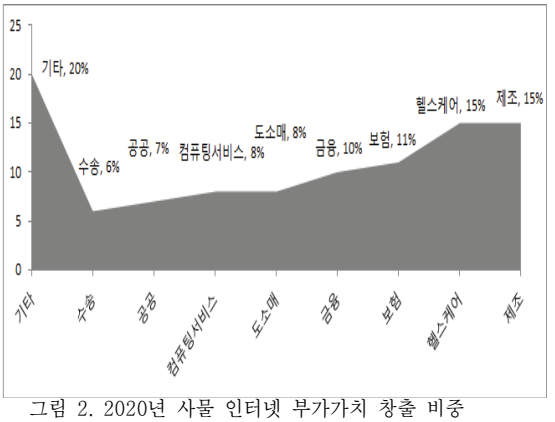

그림 2. 2020년 사물 인터넷 부가가치 창출 비중

Figure 2. Added value specific gravity of IoT

2. 초-연결 사회를 위한 보안

2.1 보안의 필요성과 정부의 대처

미래 사회 환경은 사람과 사물 뿐 만 아니라 점차 모든 것이 연결되는 사회로 확대될 전망이며, 기존의 사이버 공간 상의 위협이 현실 세계로 전이·확대 될 것이다. 따라서 보안 문제점들도 개인정보 및 공공 정보의 유출로 인한 각종 사건 사고는 물론이요, 사물들을 대상으로 하는 악의적인 공격으로 개인에게 심각한 피해를 줄 수 있으며 또한 중요한 사회 기반 시설들을 마비시킴으로써 커다란 사회 혼란 및 더 나아가 인명 손상 등을 포함한 재앙을 부를 수도 있을 것이다[5][6]. 그리고 초-연결 사회를 선도하고 이끌어 나가기 위해서는 한시라도 빨리 자율주행 자동차, 드론, 인공지능 로봇 등 주요 산업분야에서 보안위협들을 제거하기 위한 노력과 동시에 적극적인 표준화 작업이 필수적이라 생각된다[7~15].

지난 2014년 10월 사물 인터넷 관련 업무를 총괄하고 있는 부처인 미래창조과학부는 사물 인터넷과 유관 분야의 산업 육성과 안전한 사물 인터넷 사회의 구축을 위해 '사물인터넷 정보보호 로드맵'을 발표하였다. 미래창조과학부는 계획은 '사물인터넷 정보보호 로드맵'이 내재화된 IoT 기기를 만들기 위한 환경 수립과 동시에 관련 국제 시장을 이끌기 위한 9대 보안 핵심 기술의 선도적 개발과 표준화 및 이를 통한 글로벌 보안 및 융합보안 산업을 선도함으로써 국내 관련 산업계의 경쟁력을 높이고자 한다는 것이다.

2.2 주요 보안위협 사항과 고려사항

IoT 환경이 도래함에 따라 기존의 PC나 모바일 기기 중심의 사이버 환경에서와는 달리 정보보호의 대상, 주체, 방법 등에 있어 새로운 패러다임으로 접근이 필요하다. 즉, 모든 사물이 서로 연결된다는 가정 하에, 새로이 발생할 수 있는 각종 보안 위협들을 고려한 신제품의 출시를 위한 기획, 설계, 서비스 등 모든 단계에서 보안 문제를 신중하게 대비해야만 할 것이다. 또한 보호해야 할 기기의 수가 우리 일상생활의 모든 사물로 확대되고, 그 특성도 다양화 되면서 기존의 보안기술을 적용하는 것에는 한계가 있다. 그리고 다양한 분야에 IoT 응용서비스가 도입·적용되면 기존의 제조업·서비스업 등 전 산업분야에 정보보호를 반영해야 할 필요성이 생기게 될 것이다.

정부는 산업에 IoT를 적용함에 따른 보안위협을 대표적인 세 가지 산업 분야인 장비 산업 분야, 통신망 산업 분야, 플랫폼/서비스 산업 분야로 나누어 고려해 큰 고리의 정책을 세우고 있으나 하루가 다르게 변화하고 있는 초-연결 사회의 주요 산업분야에 대하여서도 구체적인 보안위협들에 대한 체계적인 분석 및 대응 방법에 대한 표준안 마련도 시급히 필요하다 할 것이다.

3. 보안 고려사항 검토 및 제안

3.1 보안 고려사항 검토

안전한 사물 인터넷 서비스를 제공하거나 받기 위해서는 보안 고려사항들에 대한 검토가 필수적이다. 정부가 발표한 IoT 장비의 단계별 보안 고려사항을 살펴보면 크게 세 단계로 보안 고려사항들을 다루었다. 모든 IoT 장비들이 설계 개발되면서부터 배포되는 단계, 설치 및 재설치 되는 단계는 물론 운영이나 관리 마지막으로 폐기되는 모든 단계에서 보안에 대한 고려가 필수적으로 고려되어야 하며 반영 되어야만 한다는 것이다.

본 논문에서는 기존의 정부 보고서에 각 단계별 추가로 고려해야 할 사항들을 연구 검토하였다. 또한 주요 산업분야 대해서는 별도로 산업의 특성에 따른 보안 고려사항을 단계적으로 구체화하여 초-연결 사회에서 발생할 수 있는 주요한 위협으로부터 안전한 생활과 서비스를 누릴 수 있도록 보완된 사항들을 기술하였다.

3.2 제안된 보안 고려사항

본 논문에서는 다음과 같은 고려사항들은 제한한다. 먼저 장비의 설계와 개발 단계에서는 장비 내에 기본적인 보안 사항들을 내포하여 설계하기 위한 전 단계로 제품의 특성과 보안 위협 정도에 따라 필요한 보안 요구사항들을 분석하여 하드웨어, 펌웨어, 소프트웨어 중 어떤 방법으로 구현할 것인가를 결정하는 단계의 삽입을 제안한다. 이를 통하여 실제 제조사의 제품 제조 가격과 보안이라는 민감한 사항들을 조정하는 사전 작업이 가능하다고 하겠다. 또한 이 단계를 거침으로써 장비의 하드웨어적인 보안 취약에 대비하기 위해 운용상 반드시 필요한 주요 코드를 펌웨어로 구현하고 실행 코드들에 대한 암호화의 수행 등의 과정을 다중으로 취함으로써 다양한 장비 운영 상황에 효과적으로 대처하도록 함은 물론 사용자에게 늘 노출되어 있는 초-연결 사회의 하드웨어를 보호하도록 하여야 할 것이다. 그리고 제품 개발 단계부터 장비 사용 시 장비에 접근 가능한 소프트웨어에 대한 사전 검토를 통하여 제품의 출시 때부터 해당 소프트웨어에 대한 보안 관련 검증과 보안을 위한 패치를 의무적으로 수행하도록 하는 방안을 제한하고자 한다.

장비의 배포 및 설치 구성 운영 단계에서는 장비의 초기 설치와 필요에 의한 재설치 시 설정되어야 하는 기본 파라미터의 값에 대한 안전성 준수 문제 해결을 위한 방안으로, 장비에 부여된 고유의 아이디를 통해 장비의 설치 및 장비 사용 과정에서 리부팅이 필요한 경우 검증된 데이터 센터의 서버에 미리 지정되어 있는 기본 파라미터의 값과 비교하는 과정을 거치도록 함으로써 필요 시 암호화된 통신을 통해 제공받도록 하는 방안을 제안한다. 그리고 소프트웨어와 소프트웨어, 소프트웨어와 하드웨어, 하드웨어와 하드웨어 사이의 보안이 함께 사용될 경우 송수신 데이터에 대해 통신 채널 및 장비에 대한 신뢰 보증 기능 제공 단계를 포함할 것을 제안한다.

마지막으로 진화하고 있는 초-연결 사회에 빠르게 대처하기 위해 파급 효과가 큰 자율주행 자동차, 드론, 인공지능 로봇 분야는 별도로 국가적인 차원에서 보안 위협을 국가 재난, 국부적인 지역 재난, 인명사고 위협, 단순 위협 등의 등급별로 구분하여 대처하도록 하여 경제적인 효과와 더불어 초-연결 사회의 안전한 삶과 서비스의 안정적 제공을 위한 표준화 작업을 병행해야 할 것이다. 또한 기존의 정보보호 운영 및 관리체계에 덧붙여 초-연결 사회의 모든 서비스를 위해 필요한 IoT 장비, 통신망 구축 장비, 각종 플랫폼에 대한 다양

한 보안 문제들과 사고에 대처하기 위한 매뉴얼 작성의 의무화를 제안한다.

4. 결 론

최근 ICT가 고도로 성장하면서 사람과 필요한 모든 사물 그리고 네트워크가 하나로 연동되는 초-연결 사회(Hyper-Connected Society)로 변화할 것이 자명해지고 있다. 이러한 환경에서는 기존의 사이버 공간 상의 위협이 현실 세계로 전이·확대될 것이며, 보안 문제점들도 개인 정보 및 공공 정보의 유출로 인한 각종 사건 사고는 물론이요, 사물들을 대상으로 하는 악의적인 공격으로 개인에게 심각한 피해를 줄 수 있으며 또한 중요한 사회 기반 시설들을 마비시킴으로써 커다란 사회 혼란 및 더 나아가 인명 손상 등을 포함한 재앙을 부를 수도 있을 것이다.

본 논문에서는 기존에 발표된 장비의 설계와 개발 단계에 제품의 특성과 보안 위협 정도에 따라 필요한 보안 요구사항들을 분석하여 하드웨어, 펌웨어, 소프트웨어 중 어떤 방법으로 구현할 것인가를 결정하는 단계의 삽입을 제안하였다. 그리고 장비의 배포 및 설치 구성 운영 단계에 장비에 부여된 고유의 아이디를 통해 기본 파라미터의 값의 안정성을 제공받도록 하는 방안을 제안하였다. 또한 두 가지 이상의 보안이 함께 사용될 경우 신뢰 보증 기능 제공 단계를 포함할 것을 제안하였다. 초-연결 사회를 선도하기 위한 보안 방안 중 하나로 본 논문에서는 보안 위협을 등급별로 구분하여 대처하도록 하는 방안과 다양한 보안 문제들과 사고에 대처하기 위한 매뉴얼 작성의 의무화를 제안하였다.

본 논문에서 제안된 사항들은 초-연결 사회에서의 보안사고 예방과 보안기술 개발 등에 필요한 자료가 될 것으로 기대하며, 점차 IoT시대에서 EoT 시대로 확장됨에 따른 새로운 보안 위협에 대한 분석과 그 위협에 대응할 수 있는 보안 요구사항 마련 및 보안 기술 개발이 지속적으로 이루어져야만 할 것이다.

References

[1] Machina Research, *http://machinaresearch.com/* March. 2016.

[2] D.-H. Kim, *Understanding of creative economic policies*, 2014.

[3] World Economic Forum, *Industrial internet of things: Unleashing the potential of connect products and services,* 2015.

[4] McKinsey & Company, *The internet of things: Mapping the value beyond the hype*, McKinsey Global Institute, 2015.

[5] Information and Privacy Commissioner, *Privacy and security by design: An enterprise architecture approach*, Canada, 2015.

[6] *Secure-coding guide*, 2014.

[7] ISO/IEC, ISO/IEC 27034-1 – *Application security - Part 1: Guideline for application security*, 2011.

[8] *CoAP(Constrained Application Protocol)*, IETF, June, 2014.

[9] *MQTT(Message Queuing Telemetry Transport)*, OASIS, April, 2016.

[10] *oneM2M Specification Release 1*, 2015.

[11] *Security Considerations in the IP-based Internet of Things*, IETF, January, 2015.

[12] Fransman, M., *The New ICT Ecosystem: Implication for Europe*, Edinburgh: Kokoro, 2007.

[13] E Andrew Lee., *Technologies Shaping the Future 'Smart' Vehicle*, FROST & SULLIVAN, 2014.

[14] Castellacci, F. *Technological Paradigms, Regimes and Trajectories*, Research Policy 37, pp.978 - 994, 2014.

[15] Chesbrough, H. W., *Open Innovation the new imperative for creating and profiting from technology*, Havard Business School Press, 2013.

초-연결 사회를 위한 보안 요구사항 분석 및 제안

김성종

극동대학교 유비쿼터스 IT학과

요 약

기술과 생산의 융합으로 다가온 스마트 사회는 기술과 생산의 혁신이 모든 분야에서 요구되고 있다. 또한 미래는 모든 사물들 사이에 통신망으로 연결되어 정보를 주고받는 초-연결 사회 시대이며, 사물 인터넷 분야는 신성장 동력 산업이 될 것이다. 하지만 사물간 상호연결이 확대되면서 이에 따른 보안위협 역시 크게 증가할 것으로 예상되며, 보호해야 할 기기들의 수가 늘어나면서 그 특성도 경량화, 저전력화, 초연결성 등으로 다양화 되면서 기기별 맞춤형 디바이스 보안기술이 요구되고 있는 시점이라 할 수 있다. 따라서 본 논문에서는 사물 인터넷 환경을 위해 필요한 보안 요구 사항들을 분석해 봄으로써, 향후 사물 인터넷의 보안 위협에 대한 대응 방안 마련에 활용할 수 있을 것으로 기대한다.

감사의 글

이 연구는 2015년도 극동대학교 교내연구비 지원에 의해 수행된 것임

Seong Jong Kim received the bachelor's degree in the Department of Electronics from the DanKook University in 1987. He received the M.S. degree and the Ph.D. degree in the Department of Electronics from DanKook University in 1989 and 1998, respectively. He was a professor in the Department of Ubiquitous IT at FarEast University since 1998. His current research interests include IoT, EoT, Security of IT and embedded system. He is a member of the KKITS.

E-mail address: ksj@kdu.ac.kr