사물인터넷 기반의 시스템을 위한 보안 취약성 및 고려사항 분석

장창환 · 조성호 · 이진협 · 김정태

*목원대학교

Analyses of Security Consideration and Vulnerability based on Internet of Things

Chang-hwan Jang · Sung-ho Jo · Jin-hyup Lee · Jung-Tae Kim

E-mail : jtkim3050@mokwon.ac.kr

요 약

사물인터넷(IoT: Internet of Things)이란 개념이 도입된 이래로 많은 ICT 관련 강대국들이 IoT 기술을 지원하고 있으며, 2014년 5월 정보통신전략위원회에서는 '사물 인터넷 기본계획'을 확정, 발표하였다 [1]. 또한 올해 2월 24일에 KISA(한국인터넷진흥원)에서는 IoT, ICT 관련기업을 지원하는 창업·벤처 지원'K-Global 프로젝트'를 공고하는 등 IoT 분야에 관한 사업이 늘어나고 있다. 이러한 사물인터넷의 다양한 서비스에 반하여 사물 간 또는 사람과 사물 간 유·무선 네트워크로 상호 연결되는 과정에서 발생하는 보안 적인 위협 요소가 발생하기 시작한다 [2]. 따라서 본 논문에서는 이러한 사물인터넷의 보안 위협이 어떤 것이 있는지, 또한 그에 따른 보안 고려사항을 분석하였다.

ABSTRACT

Recently, IoT has been supported by ICT technology with a variety of ICT powers. In May 2014, Information and Communication Strategy Committee announced the 'Basic plan for Internet of Things'. Also on Febuary 24 this SAME year, KISA(Korea Internet&Security Agency) provides many projects related to IoT, such as announcement of 'K-Global Project' for start-up and venture support related to IoT and ICT companies. In contrast to the various services of Internet of Things, when a connection is made between object-to-object or person-to-object wired and wireless networks, security threats have occurred in the process of communication. We analyzed these kinds of security threats related to Internet of things, and gave a consideration for requirement.

키워드

사물인터넷, 통신, 보안 위협, 보안 요구사항, 유비쿼터스

Ⅰ. 서 론

최근 부각되고 있는 IoT 기술은 다양한 서비스들의 서로 상이한 관리 도메인 소속일지라도 유동적으로 상호 융합되는 환경으로 정의가 가능하다 [3]. 이와 관련하여 가트너(Gartner)에서는 2020년대에는 409억대의 무선 연결 단말기 보급이 이루어 질것으로 전망하였으며 [4] 시스코(Cisco)는 20년에 25억 명의 사람들과 370억 개 이상의 사물이 연결되며, 30년에는 500억 개 이상의 사물이 초연결되는 IoE(Internet of Everything, 만물인터넷)로 진화할 것으로 예측하였다 [5]. 이와 같이 다양한 사물들은 다양한 인터넷 네트워크 기술을 기반으로 발전되는데 이러

한 다양한 네트워크 기술들과 함께 공격할 수 있는 대상 및 위협 요소가 증가되고 있다. 이것이 실생활에서는 큰 문제로 여겨지지 않지만 의료기기 등에서 특히 위협이 되고 인명 피해 뿐만이 아니라 사물이 연결되다보니 개인정보 유출·침해가 증가할 것이며, 피해량이 급격하게 증가하게 될 것으로 보인다. 비슷하게 최근 드론의 해킹을 통한 문제가 발생하고 있는데, 이것을 재밍이라고 한다. 재밍이란 기밀성, 무결성, 유효성을 통하여 드론에 공격을 하는 것인데 이는 다중 프로토콜 공격, SNR(Signal to Noise Ratio), DoS(Denial of Service), DDoS(Distributed DoS) 등을 통하여 드론의 불시착 또는 목표 변경이 이루어지고 있다.

이렇듯 많은 관심을 받는 IoT, 하지만 이로 인해 문제가 되는 IoT 보안. 이를 해결하기 위해선 이 사물인터넷의 주체가 되는 센서, 기계와 이들을 연결해주는 네트워크 기술에 관하여 수용이 되는 보안 기술의 개발 및 제공이 반드시 필수불가결하다. 본 논문에서는 사물인터넷에 대한 간단한 니해와 그에 따른 사물인터넷의 취약점 및 이를 해결하기 위한 표준화 및 대처 방안의 동향에 대해 다루고자 한다 [6].

II. 사물인터넷의 개념

사물인터넷이란 MIT Auto-ID Center 설립자인 Kevin Ashton이 1999년 사물인터넷에 대한 개념 및 용어를 처음 제안하여 사용하기 시작하였다 [7]. 이는 2005년 ITU의 “the Internet of Things” 라는 보고서를 통해 이슈화 되기 시작하였으며 2008년 글로벌 기업인 Cisco, Qualcomm, Intel 등에서 사물인터넷을 유망 아이템으로 제시하면서 큰 관심을 받게 되었다. 사물인터넷은 사물과 사물(Object to Object) 또는 사람과 사물(Personal to Object)간의 통신을 통하여 다양한 서비스를 제공하며 M2M(Machine to Machine)과 IoE(Internet of Everything)과 비슷한 기술이다. 이중 IoE와는 연결되는 개체(사물)의 범위만 다르다. M2M의 경우엔 공장, 산업시설 등 대형 시스템이 대상이 되었다면 사물인터넷의 경우엔 다른 IT 기술(Mobile, Cloud, BigData, A.I. 등)을 사용하여 다양한 사업 모델 및 서비스를 제공하고 있다. 이는 스마트워치를 통한 삼성의 헬스 케어 시스템, 한샘과 LG전자의 홈 IoT 디바이스, Google의 자율주행자동차 등 다양한 IoT 기술이 개발되고 있다. 이러한 기술 개발은 다양한 편의를 제공하게 되지만 여러 문제가 제기되고 있다. 이중 크게 물리적인 공격, 네트워킹 공격, 소프트웨어적 공격, 암호화 공격 네 가지로 나뉘게 되는데 3장에서 각각의 분류에서 어떤 것이 있는지 알아보도록 하자.

그림1. 삼성의 헬스 케어 시스템 어플리케이션 (SamsungHealth)

III. 사물인터넷의 취약점

2장에서 말했듯이 사물인터넷에서의 취약점 문제는 3가지로 나뉘게 되는데 크게 네 가지로 분류가 된다. 하지만 이 취약점 대다수는 통신 중 또는 통신 전에 공격하여 문제를 야기 시킨다.

1. 물리적 공격

물리적 공격은 말 그대로 장비 같은 것을 직접적으로 공격하는 것이다.

(1) 노드 조작: 노드 또는 하드웨어를 물리적으로 교체/조작하여 센서 노드에 손상을 주는 공격이다.

(2) RF 간섭: RFID에 사용되는 무선 주파수 신호에 잡음 신호를 전송하여 RFID 신호를 방해/간섭한다.

(3) WSN 노드 재밍: RF 간섭과 비슷하며 무선 센서 노드의 방해를 통하여 IoT 서비스의 중단을 하는 공격이다.

(4) 악성 노드 삽입: 시스템의 두 개 이상의 노드 사이에 악성 노드를 삽입/재배치하여 데이터 흐름을 제어한다.

(5) 물리적 손상: IoT 네트워크 장치를 물리적으로 손상시켜 IoT 시스템을 호스팅 해주는 지역/건물의 보안을 직접 손상시킨다.

(6) 사회 공학: 사용자를 조작하여 개인정보 추출 또는 목표에 맞추어 특정 행위를 수행한다.

(7) 수면 방해 공격: 액세스 권한 사이에 악성 코드를 물리적으로 삽입하여 노드를 손상시킨다.

2. 네트워크 공격

네트워크 공격은 개체와 개체(또는 사람) 사이에서 통신할 때 그 사이의 취약점을 이용하여 공격을 하는 방법이다.

(1) 트래픽 분석: RFID 통신 중 발생하는 데이터를 알아내 공격에 사용한다.

(2) RFID 스푸핑: RFID 신호를 스푸핑(Spoofing)하여 데이터 전송을 읽고 기록한다. 그 후 공격자는 원래 소스인 척 하여 시스템 액세스 권한을 얻는다.

(3) RFID 복제: 공격할 대상의 RFID 태그에서 데이터를 복사하여 RFID 태그를 복제한다.

(4) RFID 무단 액세스: RFID는 인증 메카니즘이 적절하지 않아 침입자의 데이터 읽기/수정/삭제가 가능하다.

(5) 싱크홀: WSN(Wireless Sensor Network) 노드에서 싱크 홀을 만들어 데이터 기밀성을 파괴하고 네트워크 서비스 거부하게 된다.

(6) Man in Middle Attack: 제한된 데이터에 액세스하고 두 센서 노드간 사이에서 도청 및 제어를 한다.

(7) 서비스 거부(DoS: Denial of Service): 다량의 트래픽 데이터를 통해 IoT 네트워크를 포화상태로 만든다.

(8) 라우팅 정보 공격: 스푸핑을 통한 침입자의 직접 공격으로 라우팅 정보를 변경/재생 시 라우팅 루프를 생성하여 트래픽 메시지 및 소스 수정, 네트워크 분할 등이 가능하다.

(9) 악의적인 공격: 노드의 신원을 주장하고 이를 가정하는 단일 노드이다. 이는 WSN 노드가 잘못된 정보를 받아들이도록 유도한다.

Layer	Threat	Requirements	Targets[1]	Approaches
Transport	Ping/ICMP flood	attacker being part of the network, ICMP	All connected devices	
	Synflood	TCP, attacker being part of the network	All connected devices	
Network	Neighbor discovery attack	Neighbor Discovery protocol	Networks using unauthenticated ND protocol	Authentication support for ND protocols
	Wormhole	Mesh networking	Multihop wireless networks	Specific hardware, time constraints on packet delivery
	Black hole	Attacker being part of the network	Multihop wireless networks	Don't use plain distance-vector based protocols.
Link	Spoofing	-	All networks, especially wireless	Packet authentication
	Eavesdropping	-	Wireless networks	Encryption
	DoS – Collision	-	Wireless networks	Use UWB, increase datarate
	DoS – Exhaustion	-	Embedded wireless networks	Link-layer Intrusion detection
	Replay protection att.	Replay protection	Multihop wireless networks	RANBAR, Tesla

그림2. 인터넷 계층별 위협 및 대응 기술 [8]

3. 소프트웨어 공격

모든 전산 시스템의 보안 취약점의 주요 원천이다. 트로이목마, 웜, 바이러스, 스파이웨어 등을 통하여 정보 도용 및 데이터 변조를 통하여 서비스 거부와 IoT 장치에 해를 끼치는 시스템이다.

(1) 피싱 공격(Phishing attack): 이메일이나 웹사이트를 통하여 사용자 자격을 스푸핑하여 기밀 데이터에 액세스한다.

(2) 악성 바이러스: 바이러스, 웜, 트로이목마, 스파이웨어, 맬웨어 등 악성 소프트웨어를 시스템에 감염시켜 다양한 문제를 야기시킨다.

(3) 악성 스크립트: 인터넷에 연결된 게이트웨이를 제어하는 사용자는 실행 가능한 Active-X 스크립트를 속여 전체 시스템 종료 또는 데이터 도난이 발생하게 된다.

(4) Dos: 응용계층을 통하여 Dos를 실행 및 공격 배포하여 네트워크의 모든 사용자에게 영향을 주게 된다. 이는 액세스 가능한 사용자를 차단할 수 있게 된다.

4. 암호화 공격(Encryption attacks)

암호화 체계를 위반하는 것에 기반 하여 IoT 시스템에 전적으로 공격하게 된다.

(1) 사이드 채널 공격: 암호화 장치의 특정기술(타이밍, 전원, 오류 및 전자기 분석)을 사용하여 암호화 키 검색이 가능하다.

(2) 암호 해독 확인: 암호문 또는 일반 텍스트 소유를 전제로 암호화 체계를 위반하여 사용되는 암호화 키를 찾는 것이다.

(3) Main in the Middle Attack: 두 사용자의 보안 통신 채널 설정 시 통신 회선 상에서 두 사용자를 위치시키게 되는데 침입자는 두 사용자의 키 교환을 별도 수행하여 간섭을 한다. 두 사용자는 느끼지 못하지만 실제로 두 사람의 공유키로 해독/암호화할 수 있게 된다 [9].

Ⅳ. 취약점 대응 현황

이처럼 사물인터넷 보안에 관하여 다양한 취약점이 있으며 보안에 따라 표준안 재정 및 보안성을 증대시키는 활동을 하게 된다. 국가적으로 많은 활동을 하고 있는데 미국, 유럽 등에서는 13년 트렌드 넷에서 CCTV보안사건 이후 공공-민간 전문가의 의견을 수렴하는 등 사물인터넷 보안 정책을 수립하기 시작하였다 [10]. 또한 IoT 계열에 급부상한 중국에서는 11년 12월중국 공업정보화부에서는 '사물인터넷 12차 5개년 계획'을 공개하고 다양한 목표를 설정하였다. 국내에서는 미래창조 과학부에서 사물인터넷 관련 보안에 관하여 15.12.0 '사물인터넷 공통보안원칙'을 발표하였다. 또한 다양한 표준화를 이루고 있다. 대표적인 인터넷 표준 단체인 IETF에선 CoAP, DICE WG표준기술, ACE WG 표준 기술 동향 등 다양한 표준안을 제시하였으며 ITU-T에서 사물인터넷 연구반(SG20)에서 표준화를 하고 있으며 ISO/IEC 두 단체에서 협의를 하여 JTC1을 설립하여 운영하며 이는 사물인터넷 작업 그룹(WG10)이 설립되어 표준화를 하고 있다 [11]. OCF(Open Connectivity Foundation)에서는 IoTivity라는 Open source Project를 통하여 오픈소스 기반의 개발 결과물을 표준으로 채택하는 특징을 가진다 [12].

Ⅴ. 결 론

이처럼 다양한 사물인터넷의 특성상 보안에 취약하며 이로 인하여 발생하는 많은 문제점이 발생하게 되며 IETF, ITU, ISO/IEC 등 다양한 표준기관부터 시작하여 Cisco 같은 글로벌 기업에서 표준 및 취약점 보안 대책을 강구하고 있다. 또한 국가적으로도 많은 대책마련에 힘을 쓰고 있는데 우리나라에서도 미래창조과학부 등 다양한 관심을 가지고 사물인터넷 표준화 및 기술력의 주도권을 가지기 위해 노력하고 있지만 지속적인 사

물인터넷에 관련한 관심을 가지고 나서야 할 것이다.

ACKNOWLEDGMENTS

This research was supported by Basic Science Research Program through the National Re-search Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (Number: 2015R1D1A09061435)

참고문헌

[1] 이효은, 홍승표, 변화성 외 9명, 정보통신기술진흥센터, “IoT 현황 및 주요 이슈”, pp.3, 2014.12.

[2] 장봉임, 김창수, “사물인터넷 보안 기술 연구”, pp.1, 2014.10.04.

[3] 강남희, “사물인터넷 보안을 위한 표준기술 동향”, pp.40, 2014.09.

[4] KISA, “사물인터넷 보안 위협 동향”, pp.3, 2014 Vol.5.

[5] 이효은, 홍승표, 변화성 외 9명, 정보통신기술진흥센터, “IoT 현황 및 주요 이슈”, pp.7, 2014.12.

[6] 손성화, 강진혁, 박경준, “드론 무선통신의 개요 및 이슈”, 2016.02.

[7] 배상태, 김진경, “사물인터넷(IoT) 발전과 보안의 패러다임 변화”, pp.45-46, 2016 Vol.14.

[8] 강남희, “사물인터넷 보안을 위한 표준기술 동향”, pp.41(그림.2), 2014.09.

[9] Ioannis Andrea, Chrysostomos Chrysostomou, George Hadjichristofi, “Internet of Things: Security Vulnerabilities and Challenges”, pp.4-5, 2015.07.06.

[10] KISA, “사물인터넷 보안 위협 동향”, pp.15, 2014 Vol.5.

[11] 강남희, “사물인터넷 보안을 위한 표준기술 동향”, pp.42-,44, 2014.09.

[12] 이종화, 김동호, “사물인터넷 기술의 국제 표준화 동향”, pp.1-2, 2016.