정 보 보 호 학 회 지
제24권 제6호, 2014. 12

M2M/IoT의 동향과 보안위협

김 영 훈*, 양 준 근**, 김 학 범***

요 약

M2M(Machine-to-Machine)/IoT(Internet of Things)는 기계 간의 통신 및 사람이 동작하는 디바이스와 기계간의 통신으로 정의하고 있으며 이 기술은 미래 ICT(Information Communication Technologies)의 핵심이 되는 기술이다. 오늘날 정보통신기술의 비약적인 발달로 언제, 어디서나 쉽게 접할 수 있는 사물지능통신(M2M) 또는 사물인터넷(IoT) 시대의 도래를 촉진하고 있지만, 다양한 단말 및 이기종 애플리케이션 등을 활용하기 때문에 발생할 수 있는 보안위협 또한 많을 것으로 예상된다. 본 고에서는 M2M/IoT의 최신동향과 동 환경에서 발생할 수 있는 보안위협들을 정의하고, 실제 사례를 통해 현재 발생하고 있는 보안위협들을 파악한 후 사례별 보안대책을 분석한다.

Ⅰ. 서 론

다리미가 알아서 옷을 다려주고, 자동인증을 통해 문을 열어주며, 토스터가 스스로 빵을 구워주는 소설 속 말도 안 되던 이야기. 오늘날 정보통신기술의 발달은 우리 주변의 모든 사물들의 지능화 및 네트워크화를 촉진하고 있으며, 이들 간의 상호통신이 가능하게 하는 유비쿼터스 환경은 더 이상 먼 얘기가 아닌 현실이 되고 있다. 유비쿼터스 환경의 도래를 더욱 가속화시키는 ICT 분야의 개념으로 상상 속의 장면을 현실화 시켜주는 사물지능통신(M2M) 또는 사물인터넷(IoT)이라 불리고 있는 이 기술은 1999년부터 회자되기 시작해 최근 들어 새롭게 떠올라 많은 관심의 대상이 되고 있다. 향후 10년간 유망할 것으로 예상하는 미래 IT 분야로 미국의 시장조사기관 가트너(Gartner)에서는 IoT를 선정한바 있으며[1], 시스코에서는 2020년 까지 전 세계 인터넷에 연결되어 있는 기기의 수가 500억대까지 증가할 것이며 수익률은 연간 22.9% 성장하여 $9,500억에 이를 것으로 전망하고 있다.[2]

우리는 지금 주변 모든 사물이 네트워크를 통해 서로 연결되는 초연결 사회(Hyper-Connected Society)로 진입하고 있는 중인 것이다. 하지만 IoT 플랫폼의 개방화, 다양한 이기종 단말/센서 및 유무선 네트워크 간의 연동 등으로 기존 보안취약점 뿐만 아니라 새로운 보안취약점이 등장할 것으로 예상된다. 이러한 보안취약점을 해결하지 못한다면 M2M 및 IoT로 인해 발생하는 심각한 보안사고를 예방하지 못할 것이다. 따라서 빠르게 발전하고 있는 IoT 서비스의 활성화를 위해서는 선도적인 보안문제의 해결이 필요할 것이다.

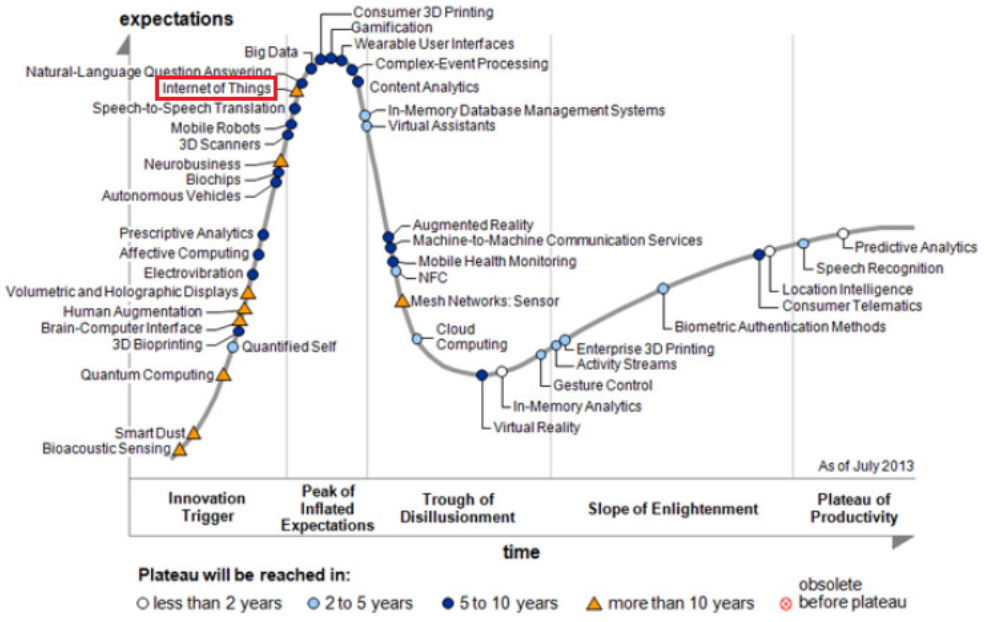
본고에서는 M2M/IoT 환경의 최신동향과 동 환경에서 발생할 수 있는 보안위협들을 정의하고, 실제 사례를 통해 현재 발생하고 있는 보안위협들을 파악한 후 보안대책을 알아본다. 본문의 구성은 다음과 같다. 2장에서는 M2M/IoT의 개념 및 정의에 대해 살펴보고, 3장에서는 M2M환경의 통신 아키텍처에 대해서 알아본다. 4장에서는 M2M/IoT의 보안위협과 함께사례를 통해 실제 보안위협을 살펴본 후 사례 별 보안대책을 도출한다. 그리고 5장에서 결론을 맺는다.

Ⅱ. M2M/IoT의 개념 및 정의

2.1. M2M/IoT의 개념 및 특징

일반적으로 사물통신(M2M)이란 '사람과 사물', '사물과 사물' 간 지능통신 서비스를 언제 어디서나 안전하고 편리하게 실시간 이용할 수 있는 미래 방송통신

* 동국대학교 국제정보대학원 (seoulkyh7@gmail.com)
** 동국대학교 국제정보대학원 (junkune@gmail.com)
*** 동국대학교 국제정보대학원 / (주)이너버스 (khb0305@dongguk.edu)



〔그림 1〕 2013 Gartner's Hype Cycle for Emerging Technologies

융합 ICT 인프라로의 진화를 의미한다. 사물통신은 기기 간 통신을 통해 수집한 정보(온도, 정량 등)를 바탕으로 유용한 정보(ex . 온도를 낮추어야 함)로 변경되어 상황을 파악하기 위해 이용된다. 사물통신의 개념이 도입된 초반에는 원격 조정이나 텔레매틱스 정도의 개념으로 인식되었고, 파생되는 시장자체도 매우 한정적이었으나, 최근 통신의 발전과 산업 현장에서의 자동화 등으로 인하여 고속 성장을 거듭하며 우리나라뿐만 아니라 전 세계적으로 사물통신이 주목받는 시장으로 성장하였다.[3]

사물통신의 특징으로는 사람이 직접 하기에 위험한 일이나 시간이 많이 소요되는 일, 또는 보안을 위한 일 등을 기계가 대신한다는 특징이 있다. 이와 같은 사물통신의 특징에 따라 사물통신은 텔레매틱스, 운동, 내비게이션, 스마트 계량기, 자동판매기, 보안서비스 등에 적용되고 있으며, 텔레비전·냉장고·세탁기 등 가전부터 자동판매기·현금인출기·자동차·건강정보를 수집하는 헬스케어 장치, 가스·전기·수도 검침기, 온도·습도 조절기까지 다양하게 사물통신 기술의 접목이 예상되고 있다.

2.2. M2M/IoT의 정의

사물통신(Machine-to-Machine Communication)은 21세기 초에 정립된 개념으로 현재 사물통신은 [표 1]과 같이 각 기관들마다 다르게 사용되고 있으며, 기술적으로는 유비쿼터스 센서네트워크(Ubiquitous Sensor Network, USN), IoT(Internet of Things) 등 여러 개념과 혼용되어 사용되고 있다. 이를 종합해보면 "지능화된 사물들이 연결되어 형성되는 네트워크상에서 사람과 사물 (물리 또는 가상), 사물과 사물 간에 상호 소통하고 상황인식 기반의 지식이 결합되어 지능적인 서비스를 제공하는 글로벌 인프라"로 정의할 수 있다.[4]

국내에서는 방송통신위원회(현 미래창조과학부)에서 2009년에 사물통신(M2M)을 사물지능통신으로 명명하고, 협의적으로 "기계간의 통신 및 사람이 동작하는 디바이스와 기계간의 통신"으로 정의하고 있으며, 광의적으로는 "통신과 ICT 기술을 결합하여 원격지의 사물정보를 확인할 수 있는 제반 솔루션"으로 정의하고 있다.[5]

각 기술적 용어는 다음과 같이 정의할 수 있다.

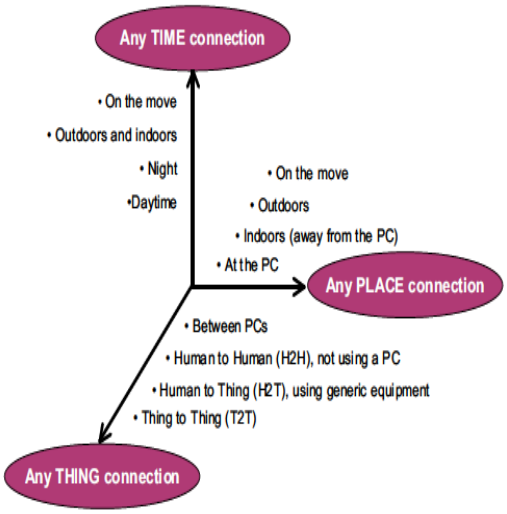
USN(Ubiquitous Sensor Network)는 지능형 센서(Intelligent Sensor)를 네트워크로 구성한 것을 말한다.[6]

IoT(Internet of Things)는 언제든지(Anytime), 어떤 장소에서(Anywhere), 누구에게나(Anyone) 어떤 것에(Anything)도 연결되는 기술이다.[7]

〔표 1〕 여러 가지 M2M(IoT) 정의[4]

기관	정의	
AIM	IoT	상호 데이터 캡쳐와 통신 수단의 사용을 통해 물리 및 가상 물체를 연결하는 글로벌 네트워크 인프라.
ITU-T	IoT	정보 사회를 위한 글로벌 인프라를 기반으로 객체(물리 및 가상)의 상호연결에 의해서 진화된 서비스를 가능하게 하는 상호 정보 통신 기술. (ITU-T.2060)
IETF	IoT	표준 통신 프로토콜을 기반으로 고유 주소 상호 연결된 개체의 세계적인 네트워크. (draft-lee-iot-problem-statement-05.txt)
EU RP7	IoT	데이터 캡쳐와 통신 능력의 개발을 통해 물리 및 가상 객체를 연결하는 글로벌 네트워크 인프라. (EU RP7 CASAGRAS)
ETSI	M2M	둘 이상의 개체 사이의 통신은 어떤 직접적인 인간의 개입을 필요로 하지 않는다. M2M서비스는 의사결정과 통신 프로세스를 자동화할 계획이다. (ETSI TS 102 689)
IEEE	M2M	가입자 단말기와 코어 네트워크의 서버간 또는 가입자 단말기간의 정보 교환은 인간의 상호작용 없이 수행될 수 있다. (IEEE 802.16p)

사물지능통신포럼은 방송통신위원회의 사물통신의 정의를 좀 더 확장하여 IoT 또한 사물통신의 다른 한 축으로 생각하고 사물지능통신을 M2M/IoT 로 표기하고 있다. 사물통신(M2M)과 IoT는 유사하다고 할 수 있으나, 사물통신은 Machine이 주체가 되어 Machine-to-Machine으로 통신하는 측면이 강한 반면, IoT는 사람을 중심으로 Things간의 연결되는 환경 측면이 강하다고 할 수 있다. IoT는 사물통신과 유사한 개념이지만 더 확장된 개념이라 할 수 있으므로 본고에서는 사물통신을 M2M/IoT로 표기하여 M2M뿐만 아니라 IoT까지 포괄하는 개념으로 정의한다.

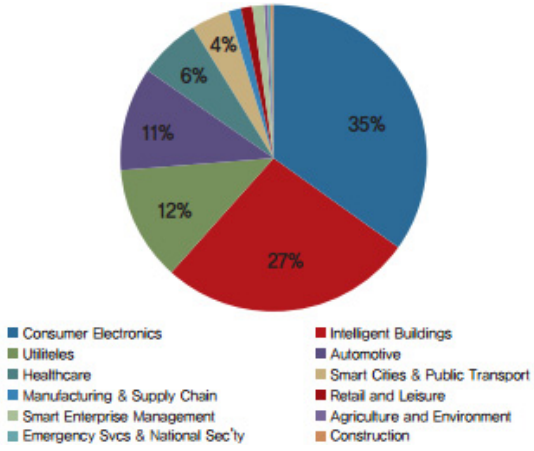


〔그림 2〕 IoT의 개념[7]

2.3. M2M/IoT 동향 및 적용분야

사물통신 기술의 발전과 사용의 증가로 인하여 전 세계 사물통신 기기는 2011년 20억대에서 2020년 120억대로 6배가 증가될 것으로 전망하고 있으며 [그림 3]와 같이 M2M 산업 중 CE, Intelligent Buildings, Utilities, Automotive, Healthcare 5개 분야가 가장 크게 성장할 것으로 전망된다.[8]

M2M/IoT의 활용이 점차 높아지면서 우리의 생활에 밀접하게 사용하고 있다. 이를 편의성, 안전성, 환경성, 예측성 측면으로 나누어 볼 수 있다.



〔그림 3〕 M2M 단말기의 주요 적용 분야[8]

2.3.1. 편의성

모바일 및 네트워크의 발달로 인해서 다양한 기기들

을 이용한 사례가 많아지면서 특히 가전/생활분야에서 이러한 기술들을 이용하는 사례가 점차 증가하고 있다.

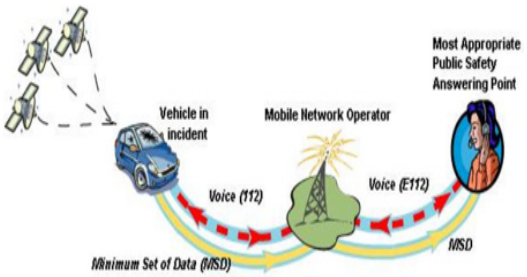
구글의 경우 오픈 API와 ADK를 모두 오픈소스로 공개하여 개발자에게 안드로이드 승인 및 라이센스의 비용을 지불하지 않고 자유롭게 개발을 할 수 있는 상황을 만들어 주면서 B2C(Buyer to Customer)의 시장에 한층 쉽게 다가갈 수 있도록 하였다. 이를 통해서 사용자 관점에서의 사용이 아닌 개발자의 관점에서도 M2M을 쉽게 적용 할 수 있도록 하여 시장접근성을 용이하게 했다.

국내에서는 스마트폰을 이용한 집안의 조명을 소등, 실내 온도조절, 가전제품 동작제어 등 가정과 M2M을 접목시킨 스마트홈(Smart Home) 시장이 점차 급성장하고 있는 추세이다.[9]

2.3.2. 안전성

유럽에서는 eCall이라는 시스템을 도입하여 사고발생 시 자동차에 설치된 사고감지 센서에 의해 자동으로 혹은 사용자가 수동버튼을 이용하여 사고접수센터(PASP)로 사고가 발생한 위치데이터를 전송한 후 사고자와 센터 운영자간에 음성채널이 연결에 상황을 즉각적으로 판단을 하는 일련의 과정으로서 2015년까지 법제화를 추진하고 있으며 2015년부터 점진적으로 실시하여 2033년에는 모든 차량에 의무 장착 법규 적용 로드맵을 구성했다.[10]

해양산업의 경우 IMO(국제해사기구)에서는 e-Navigation이라는 선박의 출항부터 입항까지의 전체과정의 안전과 보안을 위한 관련 서비스 및 해양환경 보호 증진을 위해 선박의 관련된 정보를 수집하는 체계를 2014년부터 법제화 시켰다.[11]



〔그림 4〕 유럽의 eCall 서비스

2.3.3. 환경성

최근 국내에서 쓰레기 종량제를 실시하면서 음식물 수거함 종량처리기를 많이 봤을 것이다. 이용자는 각, 동, 호수별로 발급된 RFID를 통해서 쓰레기의 배출량을 측정하고 이를 통해서 중앙관리서버는 음식물 쓰레기 배출비용에 관한 적절한 비용처리 등을 효과적으로 실시하고 있다[12]

영국에서는 의료. 위생기기업체 제니스가 자사의 차량속도를 실시간으로 파악해 좀 더 친환경적으로 운행하도록 유도하여 연료비를 22만 파운드(3.8억원) 절감하고 이산화탄소 배출을 28%줄였다.[13]

2.3.4. 예측성

브라질의 리우데자네이루 시는 기상데이터 분석을 통해 구역별 폭우 가능성을 40시간 전에 90%정확도를 예측함으로써 도로 침수 등을 사전에 대비를 한다.[14]

일본 최대 회전초밥 전문점인 스시로는 접시에 IC칩을 부착하여 언제, 어디서, 무엇이 판매되었는지에 대한 데이터를 수집하여 이를 통한 수용을 예측하여 재료의 구매 시기와 양을 결정함으로써 신선도를 관리를 하였고 각 지점 점포별 현장 직원의 배치 최적화에 활용하였다.[15]

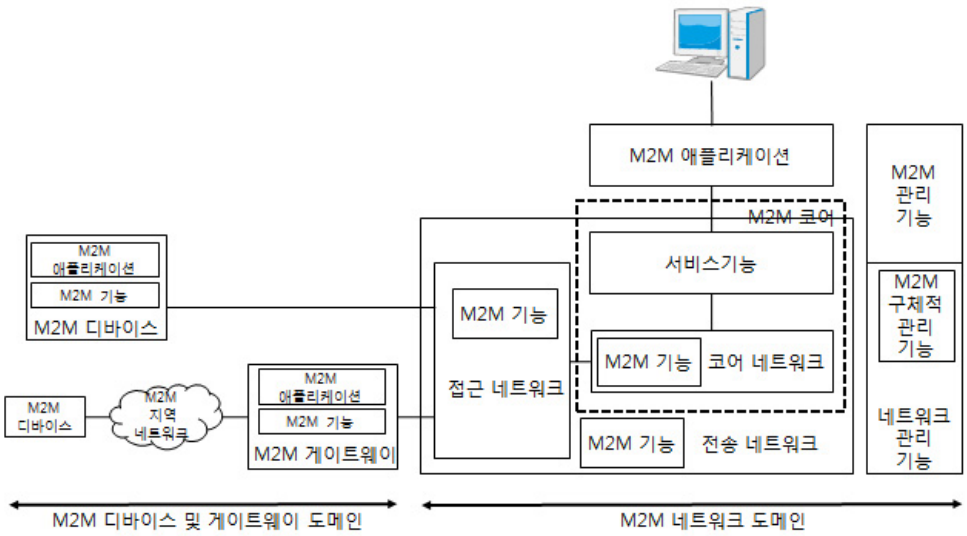
Ⅲ. M2M의 통신 아키텍쳐[16]

사물통신(M2M)의 아키텍처는 ETSI TS 102 690에서 다양한 통신기술을 통해 연결 되는 도메인으로 구성하고 있으며 M2M 디바이스(device) 및 게이트웨이(gateway) 도메인, 그리고 M2M 네트워크(network) 도메인으로 분류하고 있다.

3.1. M2M 디바이스 및 게이트웨이 도메인

M2M 디바이스 및 게이트웨이 도메인은 M2M 디바이스와 M2M 지역(Area) 네트워크, M2M 게이트웨이로 구성된다.

M2M 디바이스는 M2M 서비스 기능(Capabilities)을 사용하여 M2M 애플리케이션을 구동시키는 디바이스를 말한다. M2M 디바이스는 접근(Access) 네트워크를



〔그림 5〕 M2M 통신 아키텍쳐[16]

통해 네트워크 도메인에 직접 연결하거나 M2M 게이트웨이를 통해 네트워크 도메인에 연결한다.

M2M 게이트웨이는 M2M 디바이스와 네트워크 도메인 사이에 프록시 역할을 한다.

M2M 지역 네트워크는 M2M 디바이스와 M2M 게이트웨이 사이의 연결성을 제공하는 네트워크로써 IEEE 802.15.1, Zigbee, Bluetooth, IETF ROLL, ISA100.11a 등과 같은 PAN(Personal Area Network) 또는 PLC, M-BUS, Wireless M-BUS와 KNX와 같은 local Network를 제공한다.

3.2. M2M 네트워크 도메인

M2M 네트워크 도메인은 접근(Access) 네트워크, M2M 코어(Core) 네트워크, M2M 서비스 기능(Service Capabilities), M2M 애플리케이션, 네트워크 관리 기능, M2M 관리 기능으로 구성된다.

M2M 접근 네트워크는 M2M 디바이스 및 게이트웨이 도메인과 코어 네트워크간의 통신할 수 있는 네트워크이다. 접근 네트워크는 xDSL, HFC, satellite, GERAN, UTRAN, eUTRAN, W-LAN and WiMAX를 제공한다.

M2M 코어 네트워크는 IP와 연결성, 서비스와 네트워크 제어 기능, 다른 네트워크와의 상호연결, 로밍(roaming) 기능 등을 제공한다.

M2M 서비스 기능은 다른 애플리케이션들에 의해서 공유되는 M2M 기능을 제공하고 개방형 인터페이스를 통해 기능들을 노출하고 애플리케이션 개발을 간략하고 최적화할 수 있도록 제공한다.

M2M 애플리케이션은 서비스 로직을 구동하고 개방형 인터페이스를 통해 접근할 수 있는 M2M 서비스 기능을 사용한다.

네트워크 관리 기능은 접근 및 코어 네트워크를 관리하기 위해 요구되는 감독, 오류 관리 등의 모든 기능들로 구성된다.

M2M 관리 기능은 네트워크 도메인의 M2M 서비스 기능을 관리하기 위해 요구되는 모든 기능들로 구성된다.

Ⅳ. M2M/IoT 환경의 보안위협

사물인터넷(IoT)이라 불리는 '초연결사회'는 개인이나 사물 가릴 것 없이 모든 것이 네트워크에 연결되는 사회이다. 이 IoT 시대에 네트워크가 뚫린다면 기존 사고와는 비교가 되지 않는 초대형사고로 이어질 것으로 예상된다. 초연결사회를 지탱하는 네트워크는 보안이라는 큰 시사점을 갖고 있으며,[17] IoT 환경에서 발생할 수 있는 위협들은 기존의 정보통신환경에서 나타날 수 있는 위협들을 안고 있다. IoT 환경에서 발생할 수 있는 보안위협들을 살펴보면 다음의 [표 2]와 같다.

〔표 2〕 M2M/IoT의 보안위협

구분	보안위협
프라이버시	도청, 트래픽분석, 가로채기/방해, 기밀누설, 폐기정보수집
변조	가로채기/변경, 부인
불법 도용/접근	속임수, 권한위배, 물리적 침입, 재사용 공격, 중간자 공격
침투	바이러스, 웜, 트로이 목마
서비스 마비	자원고갈, 무결성 위배
발생 이후	절도/변경, 부인

그럼 M2M/IoT 환경에서의 몇 가지 실제 보안위협을 살펴본 후 사례별 보안 대책을 도출한다.

4.1. 실제 사례의 보안위협

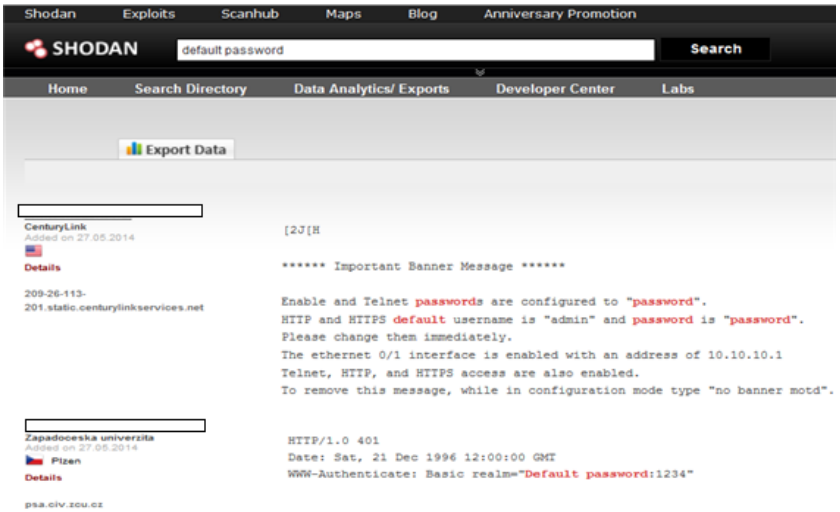
4.1.1. 검색엔진 '쇼단(Shodan)'

웹사이트 콘텐츠를 찾기 위해 웹을 수집하는 구글과 달리, 쇼단은 인터넷의 뒷구멍 채널을 항해하는데, 즉 서버, 웹캠, 프린터, 라우터 및 인터넷에 연결되어 인터넷을 구성하는 모든 것들을 찾아내는 합법적인 백도어 검색엔진이다. 쇼단에서 간단한 검색만으로 발견할 수 있는 것들을 악용할 경우, 실세계에 즉각적으로 막대한 충격을 야기할 수 있다. 이 쇼단을 이용하면 웹캠, CCTV, 보안카메라, 교통 신호, 홈 오토메이션, 난방 시스템 등 인터넷에 연결된 커넥티드 디바이스 등 인증이 필요 없는 수많은 디바이스를 손쉽게 찾을 수 있으며 심지어 핵발전소와 입자가속기의 명령 및 제어 시스템의 위치를 탐색할 수도 있다.[18]

이 쇼단을 이용하여 'default password'로 검색하면 [그림6]과 같이 아이디가 'admin'이고, 패스워드가 '1234' 혹은 'password'를 사용하는 수많은 커넥티드 디바이스들이 검색된다. 문제는 디폴트 패스워드를 사용하는 기기보다 훨씬 많은 수의 커넥티드 시스템들이 인증 자체를 전혀 요구하지 않고 있으며, 웹 브라우저를 통해 손쉽게 기기에 접속할 수 있다는 것이다.

구글과 쇼단의 차이점을 살펴보자면, 구글은 특정 텍스트를 통해 검색을 하는 반면에, 쇼단의 경우는 검색어를 통해 특정 장비를 검색하여 해당하는 장비의 HTTP Response 정보 및 IP주소를 검색해준다.

[그림 7]에서 볼 수 있듯이 쇼단에서 필터 검색(예 netcam city:seoul country:KR)을 통해 국내에 있는 IP 카메라들을 검색할 수 있으며 아무런 인증절차 없이 카메라에 접속할 수 있다. 다음의 [표 3]은 쇼단에서 사용할 수 있는 일반 필터의 종류이다. 이외에도 'scada'라는 입력만으로도 스카다 시스템을 검색할 수 있으며, 쇼단의 HTTPS 추가기능을 구매할 경우 SSL 인증버전과 SSL 인증서 공개키 길이, SSL 인증서를 받은 기관에 대한 정보, SSL 인증서를 발급한 기관에 대한 정보, 사용하는 암호 알고리즘, 암호 비트 길이, 사용하는 암호 프로토콜 등을 검색할 수 있으며 이를 통해 더욱 정확



〔그림 6〕 쇼단에서 '디폴트 패스워드(default password)로 검색한 결과

〔그림 7〕 쇼단 검색결과를 바탕으로 웹 브라우저에서 IP 카메라에 접속한 결과

한 커넥티드 기기 검색이 가능하다.

또한, 커넥티드 디바이스들은 로컬 네트워크에도 연결되기 때문에, 이 기기들을 통로로 삼아 인터넷에 연결되지 않는 다른 로컬 기기들을 확인하고 원격으로 공격하는 것 역시 가능하다. 이외에도 [표 4]과 같이 인터넷에 연결된 디바이스의 보안 취약점을 공격하는 다양한 수단들이 존재한다.[19]

앞서 설명했던 문제점들을 해결하기 위해서는 확실한 IP 주소들에만 접근을 허용하도록 인증 수단을 강구해야 하고 동시 접속의 최대치를 조정해야 하며, 커넥티드 디바이스와 로컬 네트워크를 분리해야 한다.

〔표 3〕 쇼단에서 사용할 수 있는 일반 필터

필터	설명
city	도시에 대한 필터링이다. 이 필터는 country 필터와 결합하여 사용하면 원하는 국가의 도시에서 찾을 수 있다. ex1) 서울에 있는 넷 카메라 netcam city:seoul ex2) 미국 샌디에고에 있는 Nginx서버 nginx city:“San Diego” country:US
country	국가에 대한 필터링이다. ex) 한국에 있는 웹 카메라 webcam country:KR
geo	위도와 경도를 통한 필터링이다 ex) 42.9693,-74.1224 근처의 있는 아파치 서버 apache geo:42.9693,-74.1224
hostname	특정 호스트 네임이 포함하고 있는 값을 필터링한다 예) 호스트이름에 ‘google’이 있는 Nginx서버 nginx hostname:google
net	IP를 기반으로 필터링한다. 예) IP 127.0.0.1의 모든 데이터 net:127.0.0.1
os	시스템의 운영체제를 기반으로 필터링한다 예) Windows2003에 운영되는 IIS iis os:“windows 2003”
port	포트 번호를 기반으로 필터링한다. 예) port:21
before /after	일/월/년 기준으로 이전 이후로 필터링한다 예) 2014년 6월 20일 전에 발견된 한국에 있는 아파치 서버 apache country:KR before:20/06/2014

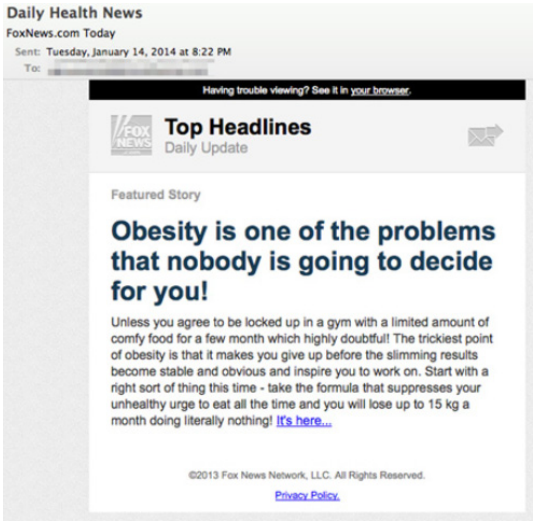
〔표 4〕 커넥티드 디바이스의 취약점 공격 수단[19]

공격방법	설명
Dynamic DNS 이용	All IP 환경이 대두되면서, 개발 업체들은 디바이스에 자체 다이나믹 DNS 서비스를 이용할 수 있는 설정을 적용하고 있는 데 이 역시 악용이 가능하다. 가령 포스캠 제품의 경우는 ‘(2개 문자, 4개 숫자).myfoscam.org’ 형식의 호스트네임을 할당 받게 되는데, 공격자들은 ‘*.myfoscam.org’라는 명령어로 호스트네임을 스캔함으로써 인터넷에 연결된 거의 모든 포스캠 카메라를 확인할 수 있음
크로스사이트 요청 위조 (CSRF)	인터페이스에 크로스사이트 요청 위조 공격을 시행하여 디바이스 관리자가 특정 링크를 얻도록 유도
Brute Force	디바이스에 대한 보안 체계가 마련되어 있지 않고 패스워드 길이 역시 12자 정도로 제한되어 있는 경우가 대부분이기 때문에 무작위 공격 가능

4.1.2. 봇넷 ‘Thingbots’

미국보안업체인 Proofpoint에 따르면 Thingbots은 인터넷에 연결되어 있는 스마트TV와 냉장고 등을 통해 Phishing과 Spam-mail을 전송한 사이버 공격 사례이다.[20] 많은 커넥티드 디바이스들은 향후 몇 년간 4배 이상 증가할 것으로 예상됨에 따라 Thingbots의 IoT 기반 공격의 증거는 기기 소유자와 기업 목표를 위한 중요한 보안 문제를 가지고 있다. 대규모 사이버 공격을 시작하는 데 사용될 수 있는 “봇넷”을 이용하여 개인용 컴퓨터를 아무도 모르게 좀비화 시킬 수 있는 것처럼, Proofpoint의 연구결과는 “thingbots”으로 홈 라우터, 스마트 가전기기 등 IoT 기기들을 악의적인 행동을 하기 위한 좀비기기로 변형하여 실제로 사용했다는 것을 밝혔다.

2013년 12월 23일 ~ 2014년 1월 6일에 전 세계적으로 기업과 개인을 대상으로 하루 3번씩 총 750,000건


Daily Health News
FoxNews.com Today
Sent: Tuesday, January 14, 2014 at 8:22 PM
To:
Having trouble viewing? See it in your browser.
Top Headlines
Daily Update
Featured Story
Obesity is one of the problems that nobody is going to decide for you!
Unless you agree to be locked up in a gym with a limited amount of comfy food for a few month which highly doubtful! The trickiest point of obesity is that it makes you give up before the slimming results become stable and obvious and inspire you to work on. Start with a right sort of thing this time - take the formula that suppresses your unhealthy urge to eat all the time and you will lose up to 15 kg a month doing literally nothing! It's here...
©2013 Fox News Network, LLC. All Rights Reserved.
Privacy Policy.

〔그림 8〕 실제 DVR을 통해 전송된 악성 url이 포함된 메일[26]

이상 발송된 이 악성 메일의 진원지는 가정용 라우터, 커넥티드 디바이스, 스마트 TV, 스마트 냉장고 등의 스마트 가전기기였다. 해당 공격자는 공격의 진원지를 노출 시키지 않기 위해 인터넷 프로토콜(IP)주소로 보내는 E-mail의 전송횟수를 10회 미만으로 제한하는 수법을 사용하였다. 또한 이러한 IoT 기기들의 암호가 노출되어 악용당한 사실도 확인되었다.

“봇넷”은 이미 해결하기 어려운 주요 보안 이슈였으며 “thingbots”의 등장은 상황을 더욱 악화시킬 수 있다. 봇넷 감염자 대부분은 감염사실을 감지할 수 없으며 이를 해결하기 위한 방법이 사실상 없기 때문이다. IoT 기기들은 일반적으로 안티스팸과 안티바이러스에 의해서 보호될 수 없기 때문에 기업들은 직원들의 메일과 악성 링크를 클릭함으로써 발생할 수 있는 분산 공격에 대비해야 한다.

4.1.3. 유아 모니터 카메라 해킹

BBC의 보도내용에 따르면 미국 텍사스의 한 가족의 집에 있는 유아 모니터링 카메라에서 음란한 소리가 들렸는데,[21] 이는 FOSCAM 제품의 취약점을 이용한 공격으로 공격자는 카메라를 해킹하여 카메라에서 음란한 목소리가 나오도록 지시한 사례이다. 아이들의 안전을 보장하기 위해 모니터링 장비를 사용하는 것은 매우 유용할 수 있지만, 인터넷에 연결되는 장비를 사용하고자 한다면, 이로 인해 증가할 수 있는 잠재적인 취약성에 대해 주의해야 한다. 이와 같은 문제를 해결하기 위해서는 인터넷에 연결되어 있는 모든 장비들의 펌웨어 및 소프트웨어를 항상 최신으로 업데이트해야 한다. 대부분의 공격은 펌웨어 및 소프트웨어에서 발견된 보안 취약점을 이용하기 때문이다. 또한, 방화벽을 설정하고 와이파이 네트워크에 연결된 유아 모니터 카메라 보안 라우터의 패스워드를 설정하는 등의 조치를 취해야 하며, 나아가 IoT 기기들을 판매하는 각 벤더사들은 보안암호 설정의 중요성을 소비자들에게 알릴 수 있는 방법을 모색해야 할 것이다.

4.1.4. Diagnostic port(OBD II)를 통한 BMW 해킹

OBD(on-board diagnostics) 포트는 차량에 내장된 컴퓨터로 배출가스 제어 부품이나 시스템 고장 등에 대해 알려주는 시스템으로 영국에서 Diagnostic port (OBD II)를 통해 자동차 도난방지시스템을 우회하여 BMW를 해킹한 사례가 있다.[22] 이는 자동차의 키 코딩 암호화가 제대로 되지 않은 취약점을 이용한 방법으로 먼저, 자동차의 침입 경보를 파괴한 후 자동차의 OBD 커넥터에 접근하고 보안되지 않거나 쉽게 복호화 되는 key codes, 프로그램, 운전거리 에 대한 정보를 수집한다.

OBD 커넥터에 연결하는 CarMD, Innova, Actron과 같은 간단한 OBD 리더기는 자동차 수리샵이나 딜러들에게 쉽게 구할 수 있다. OBD를 통한 공격방식에 대해 좀 더 자세히 보면, 공격자는 먼저 door lack을 디코딩 및 해킹하거나 초음파 경보 센서를 끄고 차의 창문을 파괴한다. 이후 OBD II 포트에 앞서 설명한 정교한 하드웨어 리더기를 연결한다. 그리고 리더기에 있는

〔그림 9〕 OBD 포트에 연결하여 스마트 키를 복제하는 데 사용되는 리더기[22]

“Preparing” 메뉴에서 “Program key”를 선택하고 빈 스마트키를 리더기에 꼽은 후에 차량 스마트 키의 디지털 ID에 접근 권한을 얻어 빈 스마트 키에 동일한 ID를 복제한다. 이제 이 복제한 스마트 키로 시동을 걸어 차량을 탈취하는 방식이다.

자동차를 해킹하는 방식에는 이러한 OBD II 포트를 통한 방식 외에도 [표 5]와 같은 다양한 방식이 존재한다.

앞서 설명한 사례 이외에도 2013년 8월에 열린 데프콘에서 2010년형 도요타 프리우스와 포드 에스케이프를 해킹하는 자동차 해킹 시연이 있었으며 이를 통해 자동차의 브레이크를 못쓰게 만들거나 핸들을 갑자기 꺾고, 엔진을 끄는 동작 등을 선보였다. 이는 자동주행 자동차는 수많은 센서에 의지해 주행하는데 정상 신호를 노트북으로 가로채어 데이터를 조작하는 방식이다.

또한, 2010년 미국 텍사스주에서 차 내비게이션을 해킹해 100여 대의 엔진과 경적을 마비시킨 사례가 있다.[23]

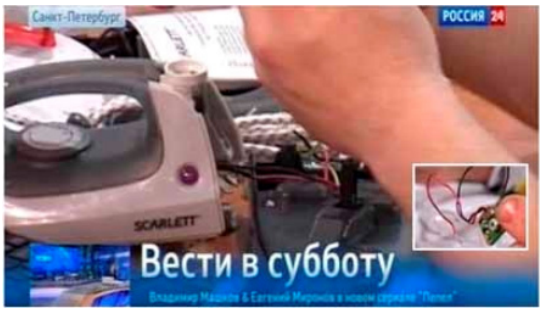
이처럼 ‘Conneted Car’로 발전하면서 자동차가 네트워크화 됨에 따라 보안 위협 또한 증가하고 있으며 이에 대비하기 위해서는 철저한 보안 위협 대응 및 보안 프로세스 도입이 필요할 것이다.

〔표 5〕 다양한 자동차 공격 방식[27]

공격방식	설명
OBD II 포트	하드웨어 리더기를 OBD II 포트에 직접 연결하여 스마트 키를 복제하고 차량을 탈취한다
Media Player	CD를 통해 펌웨어 exploit 공격을 한다
WMA parser	오디오 파일을 통해 파싱된 exploit으로 인해 차량에 임의적인 CAN 패킷을 전송한다.
Bluetooth	블루투스 프로토콜에서의 스택 오버플로우 취약점을 이용하여 안드로이드 폰에서 구동되는 트로이 목마 앱을 통해 공격한다.

4.1.5. 스마트 가전기기에 내장된 도청용 마이크로칩

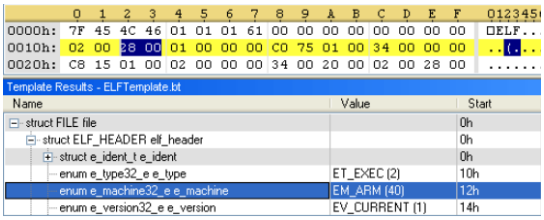
러시아에서 중국산 수입 다리미와 전기 주전자에 해킹에 활용되는 스파이 마이크로칩이 탑재돼 있는 것이 발견됐었다. 이러한 제품에 포함된 스파이 마이크로칩은 보안되지 않은 무선 네트워크에 연결할 수 있다. 일단 네트워크에 연결되면 악성코드와 스팸을 퍼뜨릴 수도 있고, 도청이나 정보 수집을 해 수집된 내용을 네트워크를 통해 해외의 서버에 전송하는 기능도 가지고 있었다. 실제로 확인된 수량만 30여개에 달하고, 확인되지 않은 수량은 훨씬 더 많을 것이라 예상된다. 이러한 시도는 다리미와 전기 주전자가 주로 쓰이는 호텔에서 각국 정상이나 주요 기업 CEO, 사업가 등을 대상으로 해킹을 하려고 했던 것으로 추측되고 있다. 또 다른 분석가에 의하면 이러한 다리미와 주전자가 배포한 악성코드에 의해 좀비 PC들이 대량으로 만들어 질 수 있었다면 이들 좀비 PC들을 통제해 훨씬 더 강력한 해킹을 수행할 수도 있었을 것으로 본다.[24]



〔그림 10〕 중국산 스파이 전기주전자[24]

4.1.6. 리눅스 달로즈 웜

IoT 기기 중 리눅스 OS를 노린 달로즈 웜은 리눅스 기반 환경에서 작동하며 무선랜카드, 셋톱박스, 보안용 IP 카메라 등을 공격할 수 있다. 시만텍의 보고서에 따르면, 리눅스 달로즈 라는 웜은 2012년 5월에 발견되된 PHP ’php-cgi’ 정보 유출 취약점(CVE-2012-1823)을 이용하는 웜으로써, 실행 즉시 임의 IP주소를 생성한 뒤 잘 알려진 ID와 password를 입력하는 방식으로 특정 기기에 접속을 시도하여 HTTP POST 요청을 보낸다.[25] 바로 이 과정에서 PHP 취약점이 악용된다. 만약 대상이 해당 취약점에 대해 패치 되지 않았다면, 악성 서버로부터 웜을 다운로드 받아 실행한 후에 다른 대상을 찾는다. 이 웜은 exploit 코드 안에 다운로드된 URL이 인텔 아키텍처를 위한 ELF binary로 하드 코딩되었기 때문에 오직 Intel x86 시스템만을 감염시키는 것으로 보인다. 아래의 [그림 11]은 ELF 헤더안의 “E_machine” 값이ARM 아키텍처에 대한 웜이라는 것



〔그림 11〕 달로즈 웜 분석[25]

을 보여준다.

이 취약점의 문제는 인터넷에 연결되어 있는 기기들은 대부분 업데이트를 하지 않거나 새로운 버전의 업데이트를 받는다고 해도 충분한 메모리가 확보되지 않거나 CPU의 성능이 저하되는 경우가 발생할 수 있다는 점이다.

4.2. 보안대책

지금까지 M2M/IoT에 대한 실제로 발생된 보안위협에 대해 알아보았다. 각 보안위협 사례에 대한 보안대책을 도출하여 다음의 [표 6]으로 정리하였다.

먼저, 쇼단과 씽봇의 사례로 살펴보면 현재 M2M/IoT

〔표 6〕 사례별 보안대책

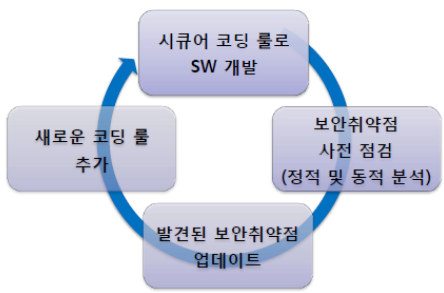
보안위협 사례	보안대책
쇼단(Shodan)과 씽봇(Thingbots)	· Access Control · 커넥티드 디바이스 인증 시스템 도입 · 강화된 패스워드 정책 · 커넥티드 디바이스와 로컬 네트워크의 분리
유아 모니터 카메라 해킹	· 최신의 F/W, S/W 업데이트 유지 · 방화벽 설정 · 강화된 패스워드 정책
BMW해킹 (자동차보안)	· 새로운 보안 프로세스 도입 · Fuzzing Test
도청용 마이크로칩	· 커넥티드 디바이스에 대한 검증
리눅스 달로즈 웜	· 커넥티드 디바이스에 대한 검증 · 최신의 S/W 업데이트 유지 · 강화된 패스워드 정책 · 다음 경로로 들어오는 HTTP POST 요청 block -/cgi-bin/php -/cgi-bin/php5 -/cgi-bin/php-cgi -/cgi-bin/php.cgi -/cgi-bin/php4

기기들의 인증 수단이 없다는 점과 인증을 도입하였지만 가장 간단한 ID/PW 인증 방식만을 도입하였다는 점이 가장 큰 문제점으로 드러나고 있다. 이를 해결하기 위해서는 강력한 디바이스 인증 시스템을 우선적으로 도입해야 하며 ID/PW 인증 방식 사용 시에는 더욱 강화된 패스워드 정책이 필요할 것이다. 또한, Access Control을 통해 아무나 접근할 수 없도록 통제해야 하며 디바이스와 로컬 네트워크간의 분리를 통해 디바이스를 통한 원격공격을 사전에 예방해야 한다.

유아 모니터 카메라 해킹 사례로 살펴보면, 이 사례는 무선 카메라인 FOSCAM 제품의 취약점을 이용한 공격으로 해당 제품뿐 아니라 다른 제품에도 취약점이 존재할 수 있기 때문에 반드시 각 벤더사에서 제공하는 F/W, S/W를 업데이트해야 하며 제로데이 공격을 막기 위한 긴급한 업데이트를 수시로 확인하여 항상 최신의 버전을 유지해야 한다. 또한, 쇼단과 씽봇과 마찬가지로 Access Control과 방화벽을 설정해야 하며 강화된 패스워드 정책이 필요하다.

OBD II 포트를 통한 BMW해킹 사례로 살펴보면, 현재 자동차 보안 공격은 점점 지능적이고 다양한 방법이 시도되고 있으며 이 공격으로 인해 생명의 위협까지 존재하기 때문에 알려진 취약점 점검만으로는 보안위협에 대응하지 못할 것이다. 이는 의도적으로 비정상적이고 변형된 랜덤 데이터를 애플리케이션에 보내 프로그램 failure를 유도하는 동적 분석의 특수한 형태인 Fuzzing Test를 통해 알려지지 않은 새로운 취약점을 탐지하여 보안 위협에 대비하여야 할 것이다. 또한, 기존의 보안 프로세스가 아닌, 아래의 [그림 12]와 같은 새로운 보안 프로세스의 도입도 필요할 것이다.

한편, 자동차 사이버 공격과 관련하여 전 세계적 차원에서 대응을 하고 있으며 올해 4월에 열린 자동차 정보 보안 국제 심포지엄 'ESCAR'에서 다양한 보안 기



〔그림 12〕 새로운 보안 프로세스[28]

술에 대한 논의가 이루어졌으며 현재 표준화 검토가 이루어지고 있는 중이다.

도청용 마이크로칩 사례로 살펴보면, 시중에 판매되고 있는 인터넷에 연결될 수 있는 모든 디바이스들에 대해 경고를 하고 있다. 스마트 가전기기의 생산 단계 혹은 생산 직후에 마이크로칩을 부착하여 악의적인 목적을 수행하려는 것을 막기 위해서는 디바이스의 무게를 측정 하는 등의 자체 검증이 필요하며, 기존의 형식적인 검증보다는 좀 더 엄격한 검증 방법이 요구된다.

리눅스 달로즈 웜 사례로 살펴보면, 유아 모니터 카메라 해킹 사례와 비슷하게 M2M/IoT 기기에 대해 최신 업데이트를 수행하지 않는다는 문제점이 있으며, 업데이트를 수행하더라도 메모리 확보 문제나 CPU 성능 저하 문제가 발생할 수 있다. 이 취약점을 해결하기 위해서는 네트워크에 연결된 모든 기기들을 검증하고 최신 버전으로 F/W와 S/W를 업데이트하고 기기의 암호를 더 강력하게 설정하고, 필요하지 않은 경우에는 게이트웨이에서 각 기기들에 대해 [표 6]에서 언급한 경로로 들어오는 HTTP POST 요청을 막아야 한다.

V. 결 론

사물통신 또는 사물인터넷 환경은 빠르게 발전하고 있으며 장비들은 점차 소형화 되고 있다. 그러나 사물인터넷의 도입이 긍정적인 효과만을 줄 수 있는 것은 아니며 우리에게 큰 위협이 될 수 있다. 이와 관련된 보안 이슈는 사물인터넷 도입의 가장 큰 진입장벽으로 여겨지고 있다. 인간의 최소개입 또는 개입이 없어도 사물끼리 통신이 가능한 기능들이 확산되면서 철저한 보안대책과 보안프로세스를 미리 준비하지 않는다면 악성코드나 악성 봇을 통해 좀비기기가 되어 우리에게 큰 피해를 입힐 것으로 예상된다. 앞으로 수많은 지능형 기기들이 서로 예측 불가능한 방식으로 통신하며 데이터를 주고받는 상황에서 데이터를 보호할 수 있는 보호대책과 보안 서비스 아키텍처에 대한 연구가 필요할 것이다. 그리고 본 고에서 설명한 M2M/IoT 환경의 보안위협 사례 외에 아직 알려지지 않은 공격 유형에 대한 연구와 함께 보안대책 연구가 필요하다. 또한 사물인터넷을 위한 오픈 소스 프로젝트가 진행되고 있는 현재 성공적인 사물인터넷 시대를 열기 위해서는 보안에 대한 많은 연구가 필요하다는 점을 강조하며 본고를 맺는다.

참 고 문 헌

[1] “2012 Gartner’s Hype Cycle for Emerging Technologies.” Gartner, August 2013.

[2] Dave Evans, "The Internet of things. How the next evolution of the internet is changing everything." Cisco White Paper, April 2011.

[3] 김유창, “기기 간 통신(M2M)의 기술 동향과 전망”, 전자부품, p.66 2009년 7월호

[4] 표철식, 강호용, 김내수, 방효찬 “IoT(M2M) 기술 동향 및 발전 전망”, IT 이슈리포트 2013-8, ETRI, p.3-4 2013.08.

[5] “사물통신 기반구축 기본계획”, 방송통신위원회, p.5 2009.

[6] “Ubiquitous Sensor Network", Technology Watch Briefing Report ITU-T, February 2008.

[7] “The Internet of Things”, ITU-T, November 2005.

[8] 고미영, “GSMA의 2020년 글로벌 커넥티드 시장 규모 전망”, KT경제경영연구소, 2012.09.

[9] "M2M/IoT시장 현황과 전망: 스마트 혁명이 M2M 시장 성장 돌파구 마련, 정책지원과 표준화 넘어야 실적인 성장기로“ EP&C, 2013.9.

[10] 김성갑, “유럽 e-Call 법제화 동향 현황” 교통안전공단 May 2013.

[11] 선웅규, "IoT/M2M 관련 산업별 시장동향“, Jan 07 2014. http://mktmaster.wordpress.com/

[12] 장미란, "음식물 쓰레기 요금, 버린 만큼만 음식물 쓰레기 종량수거기“ ㈜콘포테크, Aug 08 2013.

[13] 정미나, "영국 정부 사물인터넷에 1000억 파운드 투자“, Etn News, Jun 21 2014.

[14] 배소진, “리우데자네이루, 전례없는 ‘스마트 시티로’”, 머니투데이 뉴스, Jul 23 2014.

[15] 임태윤, "SERI 경영노트 차세대 인터넷 패러다임 M2M", p5 Aug 22 2013.

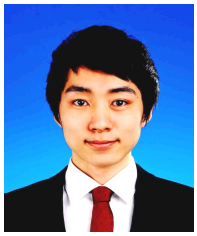
[16] “ETSI TS 102-690 v 1.1.1 Machine-to-Machine communications(M2M): Functional architecture.", ETSI, October 2011.

[17] 최희원, “보안 뚫리면 생명도 위험하다”, 나라경제, 2014년 6월호

[18] 박종훈, “심각한 보안 취약점으로 무방비 상태에 있는 사물인터넷”, 정보통신산업진흥원, 2013.5

[19] 박종훈, “사이버 공격 위험성에 노출된 비무장 상태의 스마트그리드”, 정보통신산업진흥원, 2013.6
[20] “Internet of Things(IoT) Cyberattack”, Proofpoint January 2014http://www.proofpoint.com/about-us/press-releases/01162014.php
[21] “Hacker ‘shouts abuse’ via Foscam Baby monitoring camere”, BBC August 2013 http://www.bbc.com/news/technology-23693460
[22] “Hack the diagnostics connector, steal yourself a BMW in 3 minutes”, ExtreamTech, July 2012 http://www. extremetech.com/extreme/132526-hack-the-diagnostics-connector-steal-yourself-a-bmw-in-3-minutes
[23] "Car-Hacking: Remote access and other security issues" ComputerWorld, august 2012http://www.computerworld.com/s/article/9229919/Car_hacking_Remote_access_and_other_security_issues
[24] “중국산 가전제품, 스마트폰 앱, 절대 사용금지!”, NewDaily, 2014.2 http://www.newdaily. co.kr/news/article.html?no=193744
[25] “Linux Worm Targeting Hidden Devices” Symantec, Jan.2014 http://www. symantec.com/connect/blogs/linux- worm-targeting-hidden-devices
[26] “Your Fridge is Full of SPAM” Proofpoint January 2014. http://www. proofpoint.com/threatinsight/posts/your-fridge-is-full-of-spam-part-ll-details.php
[27] “Comprehensive experimental analysis of automotive attack surfaces”, SEC, 2011.11.
[28] 이동재, “자동차 개발 시 검토해야 할 보안 대응방안”, MDS테크놀로지

〈저자소개〉



김 영 훈 (Young-Hun Kim)
학생회원

2014년 2월 : 한국산업기술대학교 컴퓨터공학과 졸업
2014년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : IoT, 사이버포렌식

양 준 근 (Jun-Keun Yang)
학생회원

2013년 2월 : 한림대학교 전자물리학과 졸업
2013년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 디지털포렌식, 암호

김 학 범 (Hak-Beom KIM)
정회원

1990년 8월 : 중앙대학교 대학원 전자계산학과 졸업(공학석사)
2001년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(공학박사)
1991년 10월~1996년 6월 : 한국전산원 주임연구원
1996년 7월~2001년 8월 : 한국정보보호진흥원(KISA) 기술표준팀장
2001년 9월~2003년 1월 : (주)드림시큐리티 상무이사
2003년 2월~2005년 3월 : (주)장미디어인터렉티브 상무이사
2008년 4월~2009년 6월 : 인포섹 (주) 수석컨설턴트
2009년 7월~2010년 12월 : 에스지에이(주) 연구소장
2011년 9월~2013년 3월 : (주)지엔에스인증원 ISMS본부장
2001년 3월~2009년 2월 : 순천향대학교 정보보호학과 겸임교수
2005년 9월~현재 : 동국대학교 국제정보대학원 겸임교수
2011년 7월~현재 : 한국정보보호학회 이사
2013년 4월~현재 : ㈜이너버스 연구소장
관심분야 : 통합로그 시스템, 빅데이터 보안, 클라우드 컴퓨팅 보안, 개인정보보호, PIMS