ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 65, No. 1, pp. 128~134, 2016
http://dx.doi.org/10.5370/KIEE.2016.65.1.128

검색엔진에 노출된 IoT 장치의 보안 위협에 대한 연구

A Study on the Security Threats of IoT Devices Exposed in Search Engine

한 경 호* · 이 성 호†
(Kyong-Ho Han · Seong-Ho Lee)

Abstract - IoT devices including smart devices are connected with internet, thus they have security threats everytime. Particularly, IoT devices are composed of low performance MCU and small-capacity memory because they are miniaturized, so they are likely to be exposed to various security threats like DoS attacks. In addition, in case of IoT devices installed for a remote place, it's not easy for users to control continuously them and to install immediately security patch for them. For most of IoT devices connected directly with internet under user's intention, devices exposed to outside by setting IoT gateway, and devices exposed to outside by the DMZ function or Port Forwarding function of router, specific protocol for IoT services was used and the devices show a response when services about related protocol are required from outside. From internet search engine for IoT devices, IP addresses are inspected on the basis of protocol mainly used for IoT devices and then IP addresses showing a response are maintained as database, so that users can utilize related information. Specially, IoT devices using HTTP and HTTPS protocol, which are used at usual web server, are easily searched at usual search engines like Google as well as search engine for the sole IoT devices. Ill-intentioned attackers get the IP addresses of vulnerable devices from search engine and try to attack the devices. The purpose of this study is to find the problems arisen when HTTP, HTTPS, CoAP, SOAP, and RestFUL protocols used for IoT devices are detected by search engine and are maintained as database, and to seek the solution for the problems. In particular, when the user ID and password of IoT devices set by manufacturing factory are still same or the already known vulnerabilities of IoT devices are not patched, the dangerousness of the IoT devices and its related solution were found in this study.

Key Words : IoT, Shodan, IoT security, IoT device hacking, Busybox

1. 서 론

시장조사 업체인 ABI 리서치사는 2013년 12월 기준으로 인터넷에 연결된 기기의 대수가 100억대에 이르며 2020년에는 300억대까지 증가할 것으로 예상했다[1].

개인 사용자 수에 의해 결정되는 PC나 인터넷에 연결되는 휴대기기와는 다르게 IoT 장치는 개인용, 가정용, 산업용으로 기존의 가전제품은 물론 의료기기, 자동차, 도로, 철도, 송전장치 등에 광범위하게 활용될 전망이며 IoT 전용 칩의 대량생산 및 기술발전에 의한 현저한 가격하락으로 대부분의 장치에 인터넷 연결 기능이 기본으로 탑재될 가능성이 크다.

이미 인텔사에서는 Quark라는 IoT 전용 프로세서를 출시하였고 그림 1과 같은 Quark 기반의 개발보드인 갈릴레오2 시리즈를 전세계에 판매하고 있다[2].

삼성의 ARTIK 시리즈등과 같이 많은 관련 제조사들 역시 Arm사의 Cortex 시리즈를 기반으로 IoT에 최적화시킨 프로세서를 출시하거나 개발 중에 있어 향후 IoT 장치 확산에 큰 영향을 끼칠 것으로 예상된다[3].

IoT 전용 칩의 개발과 수요의 증가로 인해 IoT 장치가 확산될 때 그에 따른 보안 위협 역시 증가되며 IoT시스템은 개인용 장치, 기업 내 설치된 센서 및 전자기기, 전력 및 송유인프라 등에

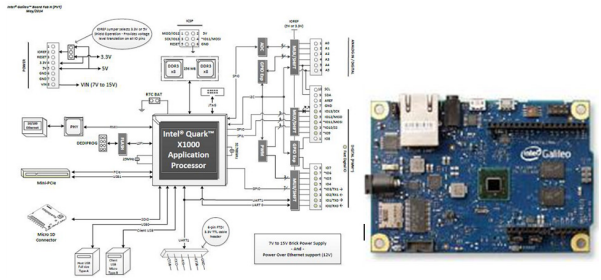

그림 1 인텔사의 Quark X1000 프로세서와 개발보드[4]
Fig. 1 Quark X1000 Processor and EVM Board

† Corresponding Author : EN Technology, Korea
E-mail : csharp1@gmail.com, ianlee@dankook.ac.kr
* Dept. of Electrical and Electronic Engineering, Dankook University, Korea
Received : October 31, 2015; Accepted : December 24, 2015

사용되며 인터넷에 연결되는 만큼 새로운 보안 문제가 발생할 수 있다.

IoT 시스템에 존재하는 다양한 보안적 위협 요소 중 IoT 장치가 인터넷에 직간접으로 노출되어 검색엔진에 의해서 정보가 수집될 때 의 문제를 파악하고 해결방법을 찾아보고자 한다.

2. IoT 장치의 확산 과 보안 위협

IoT 전용 칩이나 모듈의 출시로 인해 IoT 장치의 확산은 더욱 더 증가될 것으로 예상되고 있으며 저가로 판매되는 IoT 모듈의 확산으로 인해 기존의 고급제품에 탑재되던 인터넷 접속 기능은 전원스위치, 스마트 컵, 스텐드 등, 화분 및 전원 콘센트에 이르기까지 다양한 제품군으로 확산될 전망이다.

아래 그림 2는 $1 ~ $3에 판매되는 저가형 인터넷 연결용 모듈의 사례로써 사용된 ESP8266은 저가임에도 Wifi 모듈과 TCP/IP Protocol stack등을 포함하여 IoT 제품에 편리하게 적용할 수 있도록 구성되어 있다. ESP8266을 사용한 대부분의 모듈들은 필요한 주변회로는 물론 Wifi 안테나까지 내장하여 전원 연결 등과 같은 최소 조건만으로 기존 장치에 IoT 기능을 간편하게 추가할 수 있다.

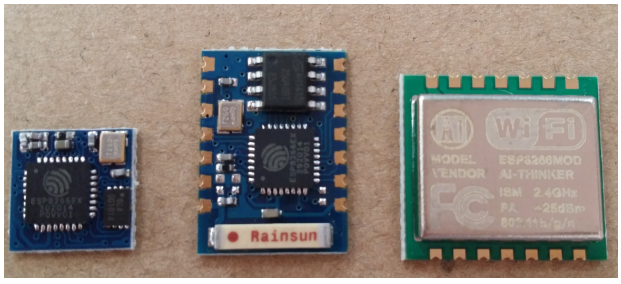

그림 2 ESP8266을 사용한 모듈
Fig. 2 ESP8266 Based Wifi Module

ESP8266 모듈은 JTAG과 같은 별도의 Debugger 장비 또는 Downloader등이 필요 없이 시리얼 포트만으로 펌웨어를 내려 받을 수 있는 구조이며 펌웨어 개발에 있어서도 무료로 사용할 수 있는 GCC 등을 활용할 수 있다. ESP8266을 사용하여 IoT 장치 또는 IoT 플랫폼을 구축하기 위한 소스는 대부분 Open source형태로 인터넷에 공개되어 있고 근래에 배포되는 ESP8266 EVM의 경우 IoT 전용 플랫폼이 사전에 탑재되어 있어 특별한 펌웨어 지식이 없어도 쉽게 IoT 장치를 개발할 수 있도록 구성되어 있다.

위와 같은 IoT 전용 칩 및 모듈의 개발로 인해 기존 Off Line으로 사용되던 기기들이 쉽게 인터넷에 연결되고 있으며 IoT 서비스 제공방식은 기존 웹서버에서 사용하는 HTTP, HTTPS, SOAP, RESTFul 프로토콜을 사용하거나 표준화된 IoT 프로토콜인 CoAP 등을 사용한다. 범용성을 갖기 위해 일반적으로 사용하는 HTTP, HTTPS, SOAP, RESTFul과 같은 프로토콜을 사용할 경우 검색엔진에 의해 IoT 장치 정보가 수집될 가능성이 증가하게 되며 IoT 장치가 외부 통신에서 사용하는 특정한 패턴을 근거로 해당 IoT장치의 정보 등이 유출될 수 있다.

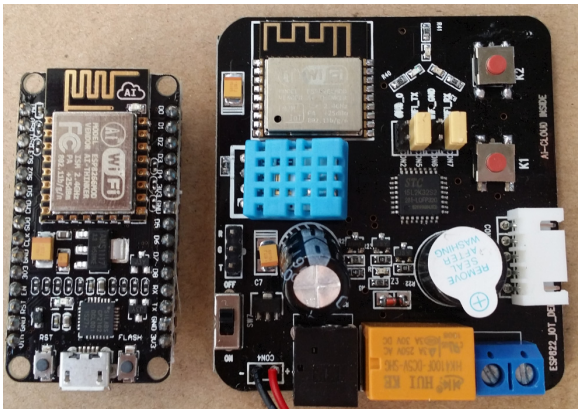

그림 3 ESP8266 모듈을 사용한 EVM 보드
Fig. 3 ESP8266 Module included EVM Board

공격자는 특별한 목적을 위하여 지정된 목표물을 공격하거나 인터넷에 연결된 수많은 기기 중 공격이 가능한 기기를 찾아 공격하기도 한다. 공격이 가능한 대상을 찾기 위해 특정 IP 주소 대역을 조사할 수 있는 포트 스캐너를 사용하기도 하지만 검색엔진을 사용할 경우 포트응답에 대한 대기시간 없이 빠른 시간에 전세계에 분포된 취약한 IoT 장치 검색이 가능하다.

기존의 범용 검색엔진과는 다른 SHODAN과 같은 IoT 장치 검색엔진의 경우 IoT 장치 탐지를 위한 전용 로봇을 사용한다. IoT 장치 전용 로봇은 IoT 장치가 사용하는 프로토콜의 요청에 응답하는 IP 주소들을 탐지하고 분석하여 서비스하는 방식으로 누구라도 해당 Site에 접속해 사용이 가능하다. 공격자는 이와 같은 검색엔진을 사용해서 인터넷에 연결된 라우터, 서버, 카메라 및 소형 장비들을 찾아 취약점을 분석할 수 있다.

IoT 및 MCU (Micro Controller Unit) 기반의 장치들은 대부분 하드웨어 내에 펌웨어로 시스템이 구성되어 있어 일반적으로 바이러스에 보다 안전하다고 알려지고 있으나 Spoofing이나 Sniffing 등과 같은 네트워크 해킹에 대해서는 일반 운영체제에 비해 안전하다고 할 수 없다. 특히, IoT 장치의 특성상 작은 메모리와 작은 가용성으로 인해 서비스 거부공격(DoS) 등에서는 일반 운영체제보다 더욱 취약할 수 있으므로 인터넷 검색엔진에 의해 취약점이 노출될 경우 보안위협이 크게 증가될 것으로 예상된다.

3. IoT 정보가 노출된 검색엔진의 취약 사례

3.1 범용 서버의 취약 검색 사례

현재는 SHODAN 뿐 아니라 SHODAN에서 파생되었거나 비슷한 유형의 사이트들이 등장하여 비슷한 유형의 서비스를 제공하고 있다. 그림 4는 www.shodan.io [5]의 메인 화면 중 일부로써 'The search engine for Internet of Things' 배너를 확인할 수 있다.

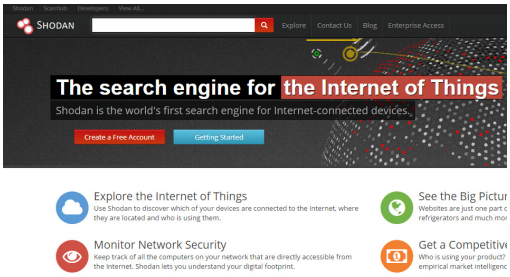

그림 4 Shodan 검색 엔진
Fig. 4 Shodan Search engine

그림 5는 www.shodan.io에서 서비스 프로그램의 보안패치가 안 되었거나 기본암호가 제거되지 않아 고난이도의 기술 없이 해킹이 가능한 상태의 장치들을 검색한 사례로 검색식 'login successful'의 결과 중 국가별, 서비스별 카운트를 나타낸 부분이다.

그림 5에서 나타난 서비스 항목 중 SMB(IPC)는 리눅스 운영체제에서 주로 사용하는 파일 공유 서비스로써 'login successful'이 표시 된 항목은 익명계정인 Anonymous 로 로그인이 성공한 것으로 일부 접근이 가능한 서버이다.

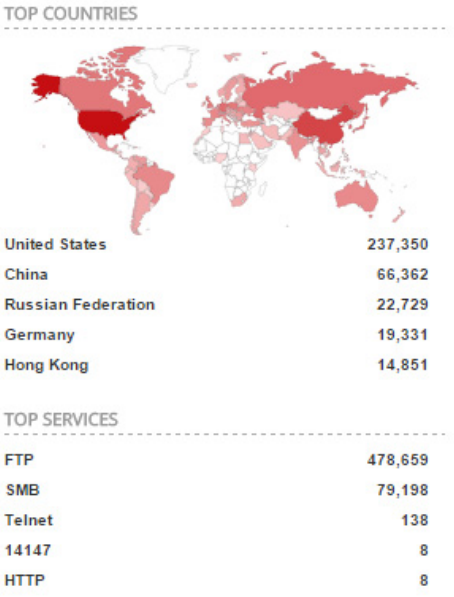

그림 5 Shodan에서 'login successful'을 검색한 사례
Fig. 5 Search result for 'login successful' on Shodan

그림 5의 'TOP SERVICES' 항목 중 SMB를 클릭했을 때 아래 그림 6과 같이 공유기능을 제공하는 IPC 포트가 인터넷에 공개된 서버 리스트가 나타나며 많은 서버들의 파일 시스템이나 공유 프린터들이 외부에 노출되었음을 확인할 수 있다.

그림 6은 검색된 79,213건 중 일부 사례이며 검색된 IP주소를 근거로 각각의 IPC서버가 미국, 캐나다 밴쿠버, 크로아티아에 위치한 서버들임을 확인할 수 있다. 마지막 항목인 크로아티아에

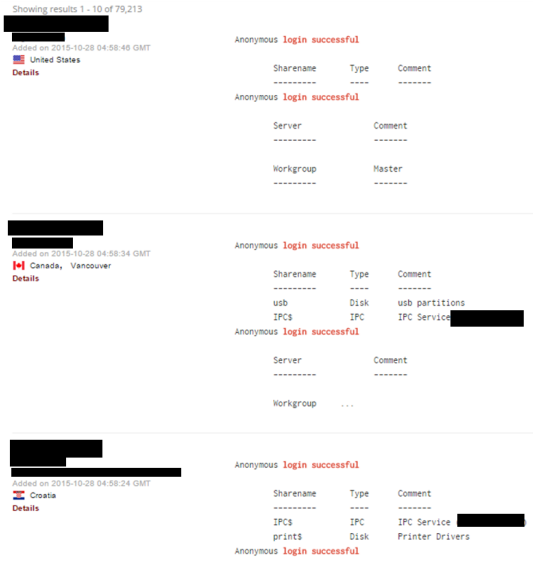

그림 6 IPC 서버 사례
Fig. 6 IPC Server List

위치한 서버를 클릭했을 때 아래 그림 7과 같이 해당 IP 주소에 대해 응답되는 포트리스트 및 각각의 포트에 대한 응답 데이터를 상세하게 조회할 수 있다.

그림 7 크로아티아에 위치한 IPC 서버의 정보
Fig. 7 Information about a IPC Server in Croatia

그림 7과 같이 서버에 대한 자세한 내역을 파악했을 경우공유 포트인 137, 445, DNS 포트인 53/tcp, 53/udp, POP3 포트인 110에 대해서 취약점을 찾아 직접 공격을 할 수도 있지만 취약점을 쉽게 찾지 못하더라도 공격자에게는 위의 HTTPD 항목과 같이 해당 서비스가 사용하는 데몬의 버전만으로도 공격에 대한

힌트가 될 수 있다.

일반 서버의 경우에는 실시간 패치, 자동 업그레이드 또는 담당자의 주기적인 관리에 의해서 업데이트되는 반면 IoT 장치와 같은 소형 임베디드 장치는 패치 및 업그레이드가 즉시 이루어질 수 없으므로 위와 같이 해킹 공격에 노출될 때 지속적인 공격의 대상이 될 수 있으며 다른 해킹을 위한 경유지로 사용될 수 있다.

3.2 검색엔진에 노출된 Embedded 장치의 검색 사례

대부분의 Embedded 운영장치를 사용하는 장치들은 Embedded 시스템의 특성으로 인해 간소화된 데몬을 사용하여 운영된다. 대표적인 Embedded용 S/W 사례로 Busybox를 들 수 있다. Busybox는 기존 Linux 시스템에서 사용되는 많은 명령어 및 데몬들을 하나의 실행파일에 구현한 프로그램으로 Embedded 시스템 개발 시 공간의 제약 등을 해소하기 위하여 많이 사용하고 있다.

그림 8은 Busybox의 공개된 기능으로써 Linux에서 자주 사용하는 명령어 대부분과 텔넷서비스, 웹서비스, FTP 서비스 등을 위한 데몬 기능이 포함됨을 알 수 있다.

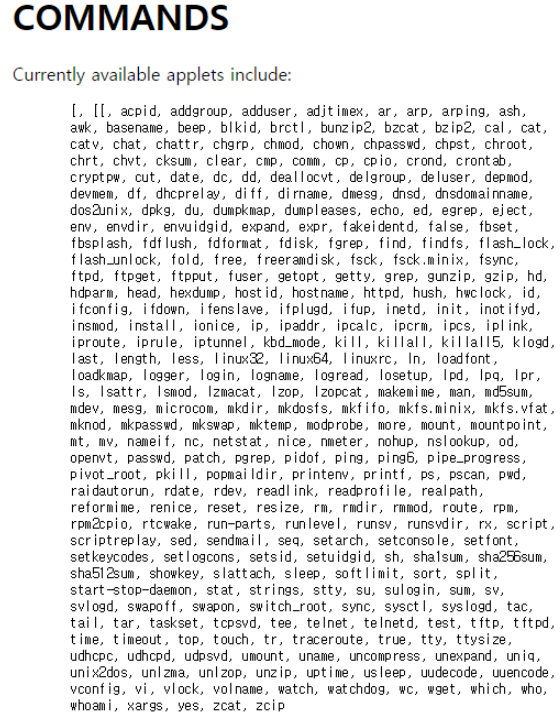

그림 8 Busybox내에 포함된 기능 목록 사례
Fig. 8 Function List of Busybox[6]

외부에서 목표 시스템을 파악할 때 가장 쉽게 사용하는 방법이 해당 시스템이 제공하는 서비스 포트에 대한 응답 메시지를 확인하는 것이고 SHODAN과 같은 검색 엔진들은 IoT 장치를 포함한 Embedded 시스템에서 사용하는 서비스에 대해 요청을 시도하고 응답 메시지를 데이터베이스화 하고 있다.

장치가 응답한 메시지를 근거로 Embedded 장치여부를 판별할 수 있으며 Busybox와 같은 데몬이 응답하는 고유 패턴을 검색식으로 사용할 경우 취약한 Embedded 시스템을 찾아낼 수 있다.

그림 9는 IoT 검색엔진 SHODAN에서 검색어 'built-in shell'으로 검색한 사례로써 검색엔진 봇이 이미 해당 시스템에 텔넷서비스를 사용하여 로그인에 성공한 것을 확인할 수 있다.

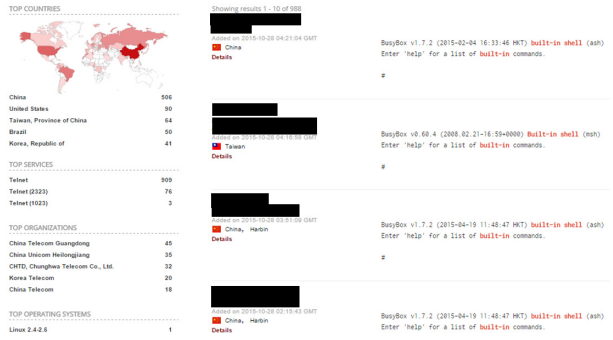

그림 9 Shodan에서 'built-in shell'을 검색한 사례
Fig. 9 Search result for 'built-in shell' on Shodan

검색에 사용된 단어인 'built-in shell'은 인터넷 공유기 나 IoT 장치 등에서 사용하는 플롯폼에서 주로 표출되는 메시지로써 일부 제품의 경우 사용자가 제품을 구매한 후 비밀번호를 설정하기 전까지 별다른 로그인과정 없이 접속만으로 Root 권한을 갖고 로그인하게 되는 위험한 shell이다.

위의 검색된 Site대부분 ID와 비밀번호 없이 접속이 가능함은 물론이고 Root권한을 사용하여 시스템을 자유롭게 제어할 수 있음이 확인되었으며 검색된 시스템 중 일부는 외부에 연결되는 공인 IP 주소와 함께 내부에서 사용하는 사설 IP 주소를 함께 사용하고 있는 것으로 확인되었다. 외부 네트워크를 경유해서 접속한 장치에서 내부 IP 주소가 발견되었다는 것은 해당 장치를 경유하여 내부 시스템까지 공격이 가능함을 나타내는 것이다.

위의 사례는 위험한 취약점 검색을 위한 검색어 중 극히 일부 사례로써 Embedded 시스템의 특성을 이용한 검색어 사용 시 인터넷에 노출된 취약한 다양한 IoT 장치를 누구나가 쉽게 찾을 수 있을 것으로 예상된다.

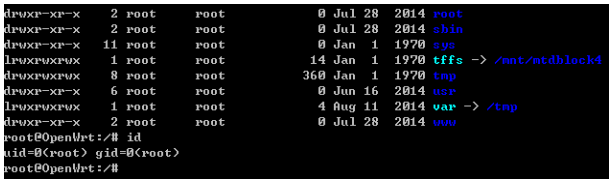

그림 10 Built-in Shell에 연결한 사례
Fig. 10 Built-in Shell Connection

3.3 IoT 장치의 특성을 이용한 취약점 공격

IoT 장치에서 사용하는 펌웨어나 IoT 장치를 구성하고 있는

임베디드 운영체제에서 보안적 결함이 발견되었을 때 빠르게 패치되거나 업그레이드될 수 없어 취약점이 지속적으로 노출될 수 있다. 특히 IoT 시스템 중 인터넷에 연결되는 매개체가 있을 때 인터넷에 상시 노출될 가능성을 갖고 있기 때문에 보안적 문제가 상존하게 된다.

이미 공개되고 알려진 취약점에 대해서는 해킹정보를 제공하는 인터넷 홈페이지는 물론 정보보안 Site에서 상세히 검색해 볼 수 있다. 대부분의 국가에서는 취약점 데이터베이스를 정형화해 외부에 공개하기도 하며 오래된 유명한 취약점의 경우에는 일반 서점에서 구입할 수 있는 보안 교제에서 '해킹사례' 등으로 쉽게 찾아볼 수 있다.

하지만 IoT 장치를 비롯한 많은 Embedded 장치는 일반적으로 사용하는 컴퓨터와는 달리 보안 패치에 대한 대응이 늦거나 심지어 보안패치가 불가능한 제품도 존재한다. IoT 장치 사용자 역시 자신이 사용하는 장치에 내장된 데몬의 서비스 버전 등을 알 수 있는 방법이 극히 드물고 IoT 장치가 원격지에 있을 경우 보안패치를 적용하기 쉽지 않은 문제점이 있다. 이미 보안적 문제가 발표되고 해결방안이 나왔으며 다양한 패치 버전이 출시되었다고 하더라도 Embedded 시스템에서는 알려진 취약점이 그대로 존재하는 경우가 상당수 발견된다.

아래는 주로 IoT 장치를 포함한 Embedded 시스템에서 사용하는 TCP/IP Stack인 lwIP를 검색한 것으로써 대부분 2012년 이전 버전을 사용하는 것을 확인할 수 있다.

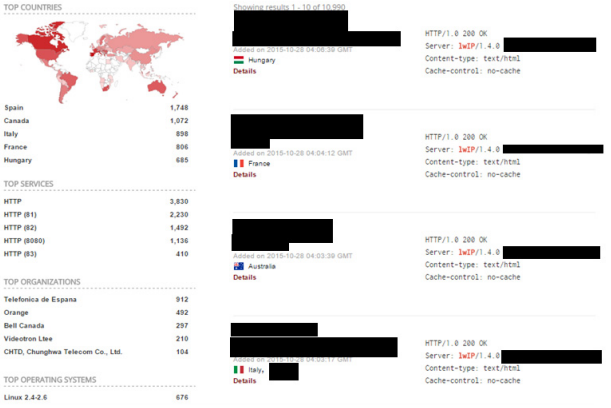

그림 11 SHODAN에서 'lwIP'를 검색한 사례
Fig. 11 Search Result for 'lwIP' on Shodan

lwIP는 버전 1.4.1을 포함한 이전 버전의 소스 중 DNS 기능을 위한 resolv.c, dns.c에 문제가 있어 Main-in-the-middle 공격이 가능함이 NIST(National Vulnerability Database)에서 2014년 11월 27일 확인되었지만 현재 SHODAN 검색엔진에서 1.4.1 버전은 물론 1.3.0 버전까지 쉽게 검색이 되고 있는 상태이다.

그림 12는 NIST에서 확인한 lwIP의 취약점 정보로써 취약정보가 발견되고 정식 등록된 시점이 2014년 11월 27일임을 확인할 수 있다.

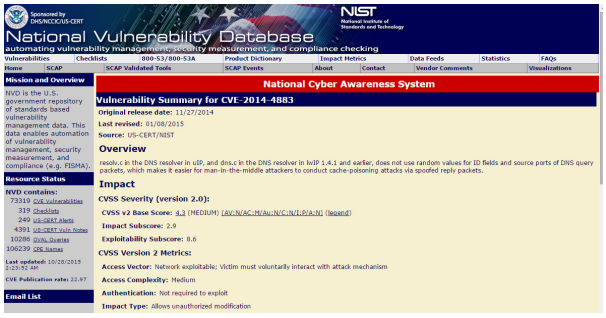

그림 12 NIST에서 검색된 lwIP에 대한 취약 정보
Fig. 12 Vulnerability summary for lwIP on NIST[7]

4. 검색엔진에 의한 IoT 장치 위협 완화 방법

IoT 장치가 직간접적으로 인터넷에 노출될 때 검색엔진 등에 의해 정보가 검색이 되고 그에 따른 보안 위협이 증가됨을 확인하였다. 사용자의 계정관리, 외부노출 장치의 관리, 네트워크 환경의 분리, 방화벽 정책등과 같은 일반적인 IoT 장치를 위한 보안사항은 기본으로 구성되어야 하며 검색엔진에 의한 IoT 장치 위협 완화 방법을 추가로 고려해야 한다.

검색엔진에 의해 의도치 않게 IoT 장치가 노출되는 것을 방지하기 위한 많은 방법 중 가장 우선해야 할 부분은 사용하지 않는 서비스 및 사용자를 제거함과 동시에 서비스 기본 포트의 변경이다. 검색엔진에서 사용하는 로봇은 빠른 검색속도를 위하여 모든 Port에 대해서 검사하기 보다는 이미 알려진 포트에 대해서 우선 검사하게 되므로 일반적으로 사용하지 않는 포트로 변경하는 방법이다. HTTP의 경우 80, 8080과 같은 일반적인 포트 이외에 16080등과 같이 사용하지 않는 포트로의 변경 시 인터넷 검색엔진이 사용하는 로봇에 의한 피 검색 속도를 늦출 수 있다.

또한, 가능하다면 암호화된 전용 프로토콜의 사용으로 검색엔진 로봇을 사전에 차단할 수 있을 것이다.

HTTP를 사용해야 되는 환경에서는 기본적으로 HTTP 서비스 루트에 robot.txt문서를 포함시키는 것도 구글과 같은 범용검색엔진을 상대하기 위한 방법 중 하나이다. robot.txt 문서 내에 검색엔진 로봇이 엑세스하지 않기를 바라는 부분을 표시 하는 것으로써 아래 그림 13의 하단 부분은 모든 검색엔진 로봇을 차단하겠다는 표현이다.

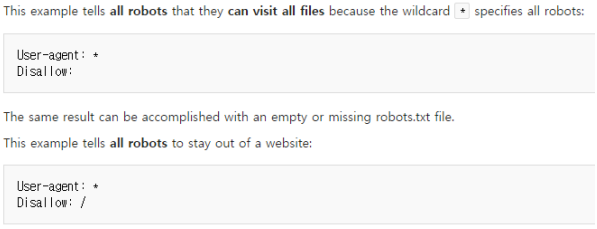

그림 13 Robot.txt 사례
Fig. 13 Examples of Robot.txt[8]

robot.txt는 주로 HTTP 프로토콜에서 사용되는 지침으로 다른 프로토콜에서는 사용할 수 없으며 HTTP 프로토콜이라도 검색엔진 로봇을 위한 지침일 뿐이므로 robot.txt에 명시한 내용이 지켜지지 않도록 구성된 로봇일 경우 robot.txt는 무시된다.

HTTP, TELNET, POP3, IPC 등 데몬이 출력하는 배너 표시에 대한 변경 역시 공격을 완화하기 위한 방법 중 하나일 것이다. 공격자는 데몬이 출력하는 패턴을 근거로 데몬의 버전 등을 유추하고 유추된 버전을 근거로 공격방법을 찾게 된다. 데몬에서 표시하는 데몬버전을 알려주는 기본 배너 변경, 커널정보를 비롯한 불필요한 정보가 출력 시 출력 설정 변경등을 통해서 최대한 IoT 장치의 정보를 숨길 수 있다[9].

5. 결 론

2020년 300억대까지 증가가 예상되는 IoT 장치가 무분별하게 인터넷 검색엔진 데이터베이스에 정형화 되었을 때 빠른 보안 패치가 어려운 IoT 장치의 특성으로 인해 보안 위협이 더욱더 증가될 것으로 예상된다. 현재 운영 중인 IoT 검색엔진인 SHODAN을 사용해서 인터넷에 연결된 IoT 장치의 보안 위협에 대해서 실험하였고 수많은 기기들이 상당히 취약한 상태로 노출되어 있음을 확인할 수 있었다.

또한 Embedded 시스템이 내부네트워크에 연결되어 있는 상태에서 라우터와 방화벽의 설정으로 외부와 연결된 경우 보안에 취약한 Embedded 시스템이 경유지로 사용되어 내부 네트워크 내에 위치한 컴퓨터나 서버 등이 공격받을 수 있음이 확인되었다. 실제로 2010년 6월 경에 발견되고 지금까지 여러 변종으로 진화되고 있는 스턱스넷(Stuxnet)이라 불리는 웜바이러스는 지멘스사의 SCADA 시스템을 감염시킨 후 장비를 감시하고 제어하는 코드를 내부에 담고 있으며 이란 핵시설이 스턱스넷에 의해 실질적 피해를 입은 경우가 있다[10].

IoT 장치가 공격받았을 때 IoT 장치가 갖는 작은 기능의 유실뿐 아니라 해당 장치와 함께 연결된 네트워크 장치들의 보안 위협이 함께 증가될 것이다. 검색엔진에 의한 IoT 장치의 보안 위협을 해소하기 위한 방법으로 기존의 일반적인 보안방법 이외에 HTTP나 TELNET, FTP 등과 같은 데몬의 서비스 Port 변경, 범용 검색엔진을 위한 Robot.txt의 활용, 서비스 데몬의 배너 변경 등을 제시하였다[11, 12].

원격지에 설치되거나 보안 패치가 다소 불편한 IoT 장치나 Embedded의 특성을 고려할 때 위와 같은 IoT 장치를 위한 보안적 기능들은 IoT 장치 개발 초기부터 함께 진행되어야 될 것으로 생각된다.

References

[1] ABI Research (2013), More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020, https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne

[2] Seong-ho Lee(2014), A Study of Forward/Reverse Connection Relay Communication for Security of IoT Devices, Dankook University

[3] Samsung artik, https://www.artik.io/hardware

[4] Intel galileo overview, http://www.intel.co.kr/content/www/kr/ko/embedded/products/galileo/galileo-overview.html

[5] Shodan Computer Search Engine, http://www.shodan.io

[6] Busybox, http://www.busybox.net/

[7] NIS, https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4883

[8] Wikipedia, Robot.txt, https://en.wikipedia.org/wiki/Robots_exclusion_standard

[9] Roland Bodenheim, Jonathan Butts, Stephen Dunlap, Barry Mullins (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. International Journal of Critical Infrastructure Protection Volume 7, Issue 2, June 2014, Pages 114-123

[10] Elsevier (2010). Stuxnet may be the work of state-backed hackers. Network Security Volume 2010, Issue 9, September 2010, Pages 1 - 2

[11] Roland Bodenheim, Jonathan Butts, Stephen Dunlap, Barry Mullins (2014). Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. International Journal of Critical Infrastructure Protection Volume 7, Issue 2, June 2014, Pages 114 - 123

[12] Jieyu Wu, Xinyu Shao, Haiping Zhu(2013). Relay node deployment based small world effect in hierarchical industrial wireless sensor networks. 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing. page 1066~1071

저 자 소 개

한 경 호 (Kyong-Ho Han)

1984년 서울대학교 대학원 전자공학과 (석사). 1992년 미국 Texas A&M University, College Station (Ph.D.). 1984～1985년 삼성휴렛팩커드 연구원. 1985～1987년 한국통신 전임연구원. 1989～1992년 Texas A&M University, Unix System Administrator & Network Analysist, 1992～1993년 한국전자통신연구원 이동통신 연구단 CDMA 개발 선임 연구원. 1993～현재 단국대학교 전자전기공학부 교수

〈관심분야〉 : 마이크로프로세서 및 Arm기반 Application, ITS, F/A System, 네트워크 통신

이 성 호 (Seong-Ho Lee)

2012년 단국대학교 정보통신 학과 (공학석사), 2015년 단국대학교 전자전기공학과 (공학박사). 현재 (주)이엔테크놀러지 대표

〈관심분야〉 : 소프트웨어 및 하드웨어 보안, Arm기반 Application, IoT Device 및 통신 프로토콜, IoT Gateway, 중계서버